UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA: INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
INGENIERA DE SISTEMAS

TEMA:

PLAN DE AUDITORÍA INFORMÁTICA PARA GRUPO EL COMERCIO C.A. CON APLICACIÓN DE LA METODOLOGÍA COBIT 4.1

AUTORA:
CARMEN ALEXANDRA BASTIDAS FIERRO

DIRECTOR:
JORGE ENRIQUE LÓPEZ LOGACHO

Quito, octubre del 2014

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE TITULACIÓN

Yo, autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de la autora.

Quito, octubre de 2014

_____

Carmen Alexandra Bastidas Fierro
CC. 1718428996

DEDICATORIA

“La esperanza hace que agite el náufrago sus brazos en medio de las aguas, aun cuando no vea tierra por ningún lado” (Anónimo).

El presente trabajo de titulación se lo dedico a Dios por iluminar mi camino; a mi mamá por su compañía y por enseñarme que a pesar de las adversidades se puede permanecer unidas; a mi hermana por haber fomentado en mí el deseo de superación, ya que llegar hasta donde hoy estoy es señal de que su preocupación sirvió.

AGRADECIMIENTO

A los docentes que me han acompañado durante el largo camino, brindándome siempre su orientación con profesionalismo ético en la adquisición de conocimientos y afianzando mi formación.

Igualmente a mi tutor, Ing. Jorge López, por su apoyo y motivación, quien me ha orientado en todo momento de manera desinteresada en la realización satisfactoria de este trabajo de titulación, que enmarca el último escalón hacia un futuro profesional; muchas gracias.

A la empresa Grupo El Comercio C.A., al departamento de Sistemas y Redacción, por la colaboración y facilidades brindadas para el desarrollo de este trabajo de titulación.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

La empresa Grupo El Comercio C.A., reconocida como periódico institucional del Ecuador, necesita de la Tecnología Informática para procesar la gran cantidad de información que genera debido al tipo de servicios que ofrece, donde el recurso tecnológico representa una gran ventaja, pero también un gran riesgo si no se cuenta con los controles necesarios que permitan la continuidad y calidad de la información al momento de aplicar cambios o efectuar nuevas adquisiciones.

El presente trabajo de titulación denominado: Plan de Auditoría Informática para Grupo El Comercio C.A., con aplicación de la metodología COBIT 4.1 tiene por objeto realizar una auditoría en los departamentos de Redacción y Tecnología usando COBIT, el cual está estructurado de la siguiente manera:

El capítulo 1 trata tanto sobre la justificación teórica de la realización del presente trabajo de auditoría como del concepto y uso del marco referencial relacionado con la administración de recursos informáticos COBIT. Además de una breve caracterización de la empresa.

El capítulo 2 procede a seleccionar los procesos y controles a auditar, a través de un marco de trabajo de cuatro dominios y 34 procesos, así como las herramientas y técnicas empleadas para conocer el grado de madurez actual de la empresa.

El capítulo 3 contiene un informe ejecutivo y un técnico que da a conocer el detalle de los principales hallazgos encontrados como parte de la auditoría.

Finalmente se presentan las conclusiones y recomendaciones obtenidas con base en la Auditoría Informática de los departamentos de Redacción y Tecnología de Grupo El Comercio C.A.

ABSTRACT

The company Grupo El Comercio C.A. recognized as institutional newspaper Ecuador needs of computer technology to process the large amount of information generated by the type of services offered, where the use of technology is an advantage, but also a great risk but is has the necessary controls to ensure continuity and quality of information when applying changes or new acquisitions.

This paper called degree: Computer Audit Plan for Trade Group CA with implementation of the COBIT 4.1 Methodology is to conduct an audit in the department of writing and technology using COBIT. The same is structured as follows:

Chapter one is as much about the theoretical justification for conducting this audit work and the concept and use of the framework related to COBIT resources management. In addition, a brief description of the company.

Chapter two proceeds to select the audit processes and controls through a framework of four domains and 34 processes, and the tools and techniques used to determine the current maturity of the company.

Chapter Three contains an executive and a technical report disclosing the details of the main findings as part of the audit.

And finally the conclusions and recommendations drawn on the computer based audit departments and Drafting Technology Grupo El Comercio C.A

INTRODUCCIÓN

El desarrollo tecnológico ha avanzado mucho en estos últimos años, por tal motivo las empresas se han vuelto cada vez más dependientes de la tecnología para manejar sus actividades de forma ágil y correcta. La disponibilidad de los sistemas informáticos se ha vuelto un aspecto crucial, por ello Grupo El Comercio C.A. ha decidido implementar un plan de auditoría que consiste en estudiar los mecanismos implantados en la organización, con el fin de evaluar sus debilidades y fortalezas, en donde el objetivo es determinar el control de la función informática, el análisis de la eficiencia de los sistemas informáticos, la verificación del cumplimiento de normativas y la revisión de la eficaz gestión de los recursos informáticos. Para ello es necesario estructurar de manera adecuada el proceso de auditoría que consiste en: planificación, ejecución y finalización de la Auditoría Informática; es por eso que se ha escogido un método práctico de investigación como COBIT 4.1, que permite la alineación de la administración de TI con los requerimientos del negocio, los cuales deben adaptarse a ciertos criterios de información como son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información. COBIT 4.1 se divide en cuatro dominios que a su vez tienen un conjunto de procesos agrupados que proporcionan la información que la organización necesita para alcanzar sus objetivos, cuyos resultados se obtendrán del análisis del nivel de madurez, que consiste en desarrollar un método de puntaje de modo que pueda calificarse a Grupo El Comercio C.A. desde inexistente hasta optimizado de (0 a 5), con lo cual el puntaje permitirá emitir conclusiones y recomendaciones útiles para mejorar el desempeño del negocio y de sus procesos estableciendo, así, medidas de control.

CAPÍTULO 1
GENERALIDADES

1.1 Planteamiento del problema

La Auditoría Informática permite la revisión y la evaluación de los controles, sistemas, procedimientos informáticos, equipos de cómputo, su utilización, eficiencia y seguridad de la organización que está inmersa en el procesamiento de la información, con el fin de lograr una utilización más eficiente y segura de la misma que servirá para una adecuada toma de decisiones.

Grupo El Comercio C.A., fundado en 1906, se ha mantenido a lo largo de estos años siempre a la vanguardia de los adelantos tecnológicos; en consecuencia, el procesamiento de la información es de vital importancia, provocando que cada vez se necesite de más control sobre los datos y los sistemas que utilizan. Por ello, la Gerencia de Tecnología quiere prestar servicios de calidad, de modo que sugiere que se realice una auditoría con el fin de plantear una línea base sobre la cual se pueda iniciar el mejoramiento.

El presente trabajo aborda principalmente: gestión del activo informático registrado en el inventario, pérdida de información por rotación o salida de personal, seguridad de los sistemas, software instalado debidamente licenciado, administración de datos, observaciones que han sido determinantes para la realización de una Auditoría Informática.

1.1.1 Hipótesis

Ayudará la Auditoría Informática en Grupo El Comercio C.A., con la aplicación de la Metodología COBIT 4.1.

Variable independiente: Auditoría Informática
Variable dependiente: Metodología COBIT 4.1

1.1.2 Objetivos.

1.1.2.1 Objetivo general

- Realizar un Plan de Auditoría para el Grupo El Comercio C.A., con aplicación de la Metodología COBIT 4.1

1.1.2.2 Objetivos específicos

- Recopilar información de la seguridad física y lógica de los diversos ambientes de procesamiento de la misma.
- Estudiar y seleccionar los procesos del marco de trabajo COBIT apropiados para Grupo El Comercio C.A.
- Realizar la auditoría, estableciendo el grado de madurez actual de acuerdo con los modelos de COBIT.
- Elaborar y entregar el Informe de la Auditoría Informática, considerando todo los hallazgos encontrados.

1.1.3 Justificación del tema

A escala internacional, la Auditoría Informática se ha constituido en un pilar fundamental del desarrollo de las organizaciones de muy variadas razones sociales, lo cual ha motivado que los diversos procedimientos y sistemas, como la estructura física, por ejemplo, deben estar supeditados a los correspondientes controles de calidad.

Tomando en cuenta que gran parte del tiempo laboral se ocupa en el uso de la tecnología, como herramienta indispensable de trabajo, los funcionarios de Grupo El Comercio C.A. han considerado de gran interés e importancia para la empresa, propiciar una investigación de este tipo en los departamentos de Redacción y Tecnología.

Este procedimiento estará encaminado a recoger, agrupar y evaluar evidencias para determinar si el sistema de información salvaguarda el activo de la entidad, mantiene la integridad de los datos, cumple eficazmente con los fines de la organización y utiliza de manera eficiente los recursos dispuestos para la seguridad informática.

Con los resultados obtenidos, se espera alcanzar un informe que ayude a rectificar los errores, en caso de que los hubiese, o bien optimizar el funcionamiento y desarrollo de los departamentos auditados y, con ello, facilitar la toma de decisiones que convengan a las necesidades y presupuesto de la empresa, en la perspectiva de excelencia en la productividad informática.

Entre las consideraciones para escoger el estándar COBIT 4.1 se debe mencionar, principalmente, que este procedimiento incluye las mejores prácticas en tecnología, alineadas al gobierno de la TI (Tecnología de la Información), junto a guías de auditoría. Se apoya en la evaluación de 34 procesos definidos por esta metodología y agrupados en cuatro dominios, a saber:

- Planear y organizar.
- Adquirir e implementar.
- Entregar y dar soporte.
- Monitorear y evaluar.

Posteriormente, se presentan las respectivas recomendaciones que sugiere COBIT 4.1.

De esta forma, Grupo El Comercio C.A. espera obtener eficiencia, eficacia, rentabilidad y seguridad en cada uno de sus procesos. La investigación tendrá lugar bajo lineamiento y herramientas estándares de COBIT 4.1.

1.1.4 Alcance.

Grupo El Comercio C.A. es un medio de comunicación con visión a **s**er la mejor empresa periodística del país. Por lo que es necesaria una auditoría que permitirá analizar, verificar y exponer debilidades, mediante el uso de técnicas de recolección de datos. Como resultado se obtendrá un informe con el detalle de los hallazgos de vulnerabilidades o inexistencia de controles, los riesgos que pueden ocasionar y los planes de mitigación recomendados.

Con los hallazgos de vulnerabilidades, los riesgos asociados a estas y las recomendaciones emitidas para mitigar las mismas, Grupo El Comercio C.A. podrá aceptar o no las sugerencias para definir un plan de mejora de la aplicación auditada.

1.1.4.1 Delimitación de la investigación

Delimitación de contenido: el proyecto de investigación planteado sigue una metodología de auditoría general y los criterios del modelo COBIT, que dan un marco de referencia y de trabajo estandarizado, que involucra documentos con temas clasificados a través de dominios, procesos y actividades.

Las áreas que serán auditadas son la de Redacción y Tecnología, en las cuales se usará un grupo de matrices o encuestas para trabajar con ellas durante el proceso de auditoría.

Se ha decidido realizar una selección de los procesos que abarca la metodología COBIT:

- **PO1** Definir un plan estratégico de TI.
- **PO2** Definir la arquitectura de la información.
- **PO3** Determinar la dirección tecnológica.
- **PO6** Comunicar las aspiraciones y la dirección de la Gerencia.

- **AI1** Identificar soluciones automatizadas.
- **AI2** Adquirir e implementar software aplicativo.
- **AI3** Adquirir y mantener infraestructura tecnológica.
- **AI4** Facilitar la operación y el uso.
- **DS4** Garantizar la continuidad del servicio.
- **DS5** Garantizar la seguridad de los sistemas.
- **DS9** Administración de la configuración.
- **DS10** Administración de problemas.
- **DS11** Administración de datos.
- **DS12** Administración del ambiente físico.
- **DS13** Administración de operaciones.
- **ME1** Monitorear y evaluar el desempeño de TI.

Delimitación espacial: Seguridad informática.

Delimitación temporal: La investigación se llevará a cabo durante un año. El progreso del proyecto de investigación que se basa en una Auditoría Informática está dado con la culminación de un informe ejecutivo, considerando todo los hallazgos encontrados.

1.2 Caracterización de la empresa

1.2.1 Descripción de la empresa

Grupo El Comercio C.A. fue fundado en Quito, el 1 de enero de 1906, por los hermanos Carlos y César Mantilla Jácome. El diario nació como un periódico independiente, liberal, pero no partidista, dedicado a servir los intereses del país. A lo largo de sus 106 años de vida, esta empresa ha sido testigo y protagonista de la historia ecuatoriana, permanente impulsor de las grandes realizaciones nacionales y gran defensor de la democracia y las libertades públicas e individuales. Su inquebrantable defensa de la libertad de expresión le representó más de una clausura.

A través de su larga trayectoria, este medio de comunicación ha sido parte del coexistir nacional, como informador y conciliador en los acontecimientos históricos de la sociedad ecuatoriana. Así también, ha sido partícipe del desarrollo comunitario haciendo énfasis en los valores que identifican a nuestra colectividad.

La mejora constante del periodismo ecuatoriano, así como de la publicidad, fueron impulsados por este medio de comunicación, a través de una constante capacitación de su talento humano, así como también por su preocupación en el constante desarrollo de su tecnología en el área gráfica.

Grupo El Comercio C.A. se ha mantenido a lo largo de estos años siempre a la vanguardia de los adelantos tecnológicos, así como de las nuevas corrientes y tendencias periodísticas, sin alejarse de los postulados ideológicos que han sido la esencia de su presencia y credibilidad, gracias a la independencia y desvinculación con otras actividades que no sean sólo las periodísticas. Por ello ha recibido un sinnúmero de reconocimientos de prensa, tanto periodísticos y de diseño como de impresión.

Además, esta compañía forma parte de Grupo de Diarios América (GDA), que es un consorcio exclusivo integrado por los 11 periódicos independientes con más influencia en Latinoamérica: La Nación (Argentina), O Globo (Brasil), El Mercurio

(Chile), El Tiempo (Colombia), La Nación (Costa Rica), El Comercio (Ecuador), El Universal (México), El Comercio (Perú), El Nuevo Día (Puerto Rico), El País (Uruguay) y El Nacional (Venezuela).

El GDA es considerado, actualmente, como el medio más eficaz de comunicación en Latinoamérica. Esto gracias a que cuenta con aproximadamente 3 000 periodistas en 25 naciones y 15 años de experiencia y credibilidad como ente informativo.

Portafolio de negocio: Las marcas de Grupo El Comercio C.A. son administradas en concordancia con las directrices señaladas por los valores empresariales establecidos. Este cuidadoso manejo ha generado un sólido posicionamiento entre la audiencia.

El amplio portafolio, orientado a diferentes públicos, acompaña con información y entretenimiento a lo largo del día y en tiempo real. Así, las marcas que se manejan en la empresa se han vuelto multiplataforma (medios impresos, digitales, redes sociales y radios) logrando una cobertura nacional e internacional.

Medios impresos

Los contenidos impresos son producidos con altos estándares de calidad, profesionalismo y cuidadosamente administrados por la empresa; están dirigidos a diversas audiencias.

- **El Comercio:** Es un matutino de tamaño estándar, con circulación nacional diaria.

Es el único periódico ecuatoriano miembro del GDA (Grupo de Diarios América) y del IFRA (Color Quality Club). Ha obtenido varios premios internacionales de periodismo y otros reconocimientos mundiales por su calidad de impresión.

- **Últimas Noticias:** Vespertino con información ágil y concisa acompañada de un gran soporte gráfico, con los objetivos de satisfacer los requerimientos de los lectores.

- **Ultimitas:** Revista semanal infantil de Últimas Noticias que constituye un importante apoyo al aprendizaje y la actividad escolar: lenguaje, matemática, historia, juegos de ingenio, actividades escolares…

- **Semanario Líderes:** Los emprendedores, los empresarios y los estudiantes universitarios interesados en informarse sobre nuevas estrategias de mercado encuentran en esta revista de economía y negocios todo un ámbito de oportunidades de inversión e ideas innovadoras. Los grandes temas económicos de actualidad en el Ecuador y el mundo también tienen su espacio.

- **Familia:** Su contenido es altamente valorado por los lectores debido a su utilidad y practicidad. Los temas de esta revista dominical son disfrutados por todos los miembros de la familia.

- **Súper Pandilla:** Revista infantil del Grupo El Comercio C.A., con diseño y contenido acordes con los gustos de los niños de esta generación.

- **Carburando:** La más completa información técnica y deportiva del automovilismo nacional e internacional.

- **EducAcción:** Revista mensual dirigida a los docentes del país, con temas pedagógicos de interés para aplicarlo en las aulas de clase; también posee información de materia legal.

Impresión comercial

Este departamento pone a servicio de la comunidad impresiones en alta calidad de todo tipo de tirajes publicitarios. Además, ofrece impresión de libros para las editoriales de materiales educativos, didácticos e informativos, para toda América Latina.

- **Material didáctico:** libros, cuadernos, mapas, láminas educativas.
- **Material POP:** afiches, catálogos, volantes, folletos, calendarios.
- **Impresos:** revistas, suplementos, insertos, coleccionables, papel de regalo.

Unidad digital

Desarrolla alternativas de soluciones de contenido multimedia, acordes con los nuevos requerimientos del exigente mercado. Forman parte de esta división de negocio las ediciones digitales de los distintos productos, los servicios de noticias y los nuevos portales de clasificados en Internet.

- **El Comercio (www.elcomercio.com):** Todo el acontecer nacional y mundial, de manera inmediata, con permanente actualización de la información: gráficas, audios, videos. Además, muchos recursos interactivos para todo público.
- **Revista Líderes (www.revistalideres.ec):** Actualización permanente de noticias, entrevistas, indicadores económicos, casos de éxito y mucho más es la oferta de Líderes en la web.

- **Revista Familita (www.revistafamilia.com.ec):** Información digital del impreso, con notas más ampliadas y otros recursos familiares, como reportajes, consejos, historias exclusivas de esta página.

- **Ultimas Noticias (www.ultimasnoticias.ec):** Funciona como un gran blog. Sus principales temas, tratados en formato multimedia, tienen que ver con la comunidad quiteña, los deportes, la seguridad y el entretenimiento. La comunidad puede también contar directamente sus noticias, dejar sus comentarios, enviar sus fotografías.

- **EducAccion (http://educaccion.elcomercio.com):** En formato PDF, aquí se encuentra toda la información digitalizada, de esta revista mensual, dirigida a todos quienes están involucrados en la enseñanza pedagógica.

- **Compra Ya (www.compraya.ec):** Es un portal web que garantiza precios inigualables con descuentos que van desde el 50% al 90% en ofertas de salud, belleza, restaurantes, entretenimiento, tecnología, turismo, etc.

Empresas relacionadas

- **Radio Quito:** Con más de siete décadas de trabajo constante, esta emisora mantiene su liderazgo de audiencia a través del entretenimiento, la información y la educación en sus diferentes programas diarios.

- **Radio Platinum:** Estación dirigida al adulto contemporáneo, con programación selecta. Dos noticieros, resumen de noticias, boletines informativos cada 60 minutos, revistas de variedades con temas de contenido profundo y una gran selección de éxitos musicales.

- **EcuadoRadio:** Es la agencia de noticias más importante del país. Profesionales de la comunicación laboran permanentemente para ofrecer información veraz y de primera mano a los oyentes de las radios Quito y Platinum.

Figura 1. Productos y marcas del Grupo el Comercio C.A.

Fuente: Grupo El Comercio C.A.

1.2.2 Ubicación de Grupo el Comercio C.A.: Calle El Tablón 11515 y Av. Pedro V. Maldonado.

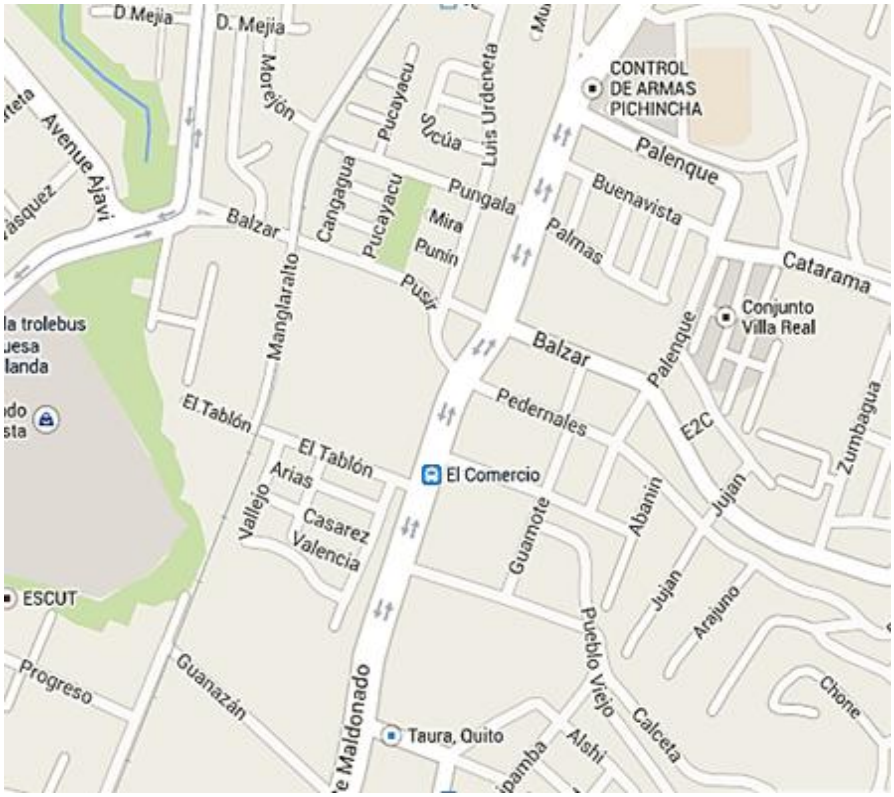


Figura 2. Localización de la empresa Grupo El Comercio C.A.

Fuente: www.google.com.ec/maps/place/Quito/@-0.2701401,-78.5278598,17z/data=!4m2!3m1!1s0x91d59a4002427c9f:0x44b991e158ef5572

1.2.3 Visión

Ser la mejor empresa de medios de comunicación del país, focalizada siempre en:

- El desarrollo de proyectos periodísticos de calidad.
- Propuestas innovadoras para los anunciantes.
- Proactividad frente a los cambios de la industria.
- Ser una empresa rentable y en continuo crecimiento.
- Brindar oportunidades de desarrollo a su gente.

1.2.4 Misión

Contribuir diariamente al desarrollo de un Ecuador libre, democrático y solidario, mediante contenidos de valor para las distintas audiencias y soluciones de comunicación para los anunciantes.

1.2.5 Valores

- ✓ **Independencia:** Un medio se debe, sin atenuantes, a los lectores.
- ✓ **Integridad:** Ética y responsabilidad en el trabajo periodístico y en todas las actividades.
- ✓ **Innovación:** Indispensable para atender las cambiantes necesidades de audiencias y anunciantes.
- ✓ **Calidad:** En productos y servicios al cliente y en la relajación con nuestra gente.

1.2.6 Objetivos estratégicos

- Lograr que una cuarta parte de los ingresos de la empresa provenga de los negocios digitales, de impresión comercial, optativos y nuevos proyectos.
- Elevar la productividad continuamente en todas las áreas y aplicar procesos periodísticos de vanguardia, para modernizar las redacciones.
- Reinventar los productos actuales del portafolio y crear nuevos para aumentar, de manera sostenible, la audiencia de periódicos y revistas, atendiendo competentemente la nueva dinámica de los anunciantes. Emprender un importante desarrollo en el mercado digital de forma rentable.
- Cuidar las marcas, asegurar los resultados financieros y cumplir las normas de Buen Gobierno Corporativo. (Comercio, 2012, pág. 9)

1.2.7 Estructura organizacional

Figura 3. Diagrama organizacional del Grupo El Comercio C.A.

Elaborado por: Carmen Bastidas, tomado del reporte de responsabilidad social corporativa 2012

1.2.8 Análisis FODA.

Tabla 1

Análisis FODA de la empresa Grupo El Comercio C.A.

Fortalezas	Debilidades
• Alta calidad de impresión. • Portafolio bien posicionado. • Mercado claramente definido. • Características especiales del producto que se oferta. • Reconocida marca en el mercado nacional e internacional. • Ediciones digitales de los distintos productos del portafolio. • Es un medio con un alto nivel de credibilidad	• Convergencia digital. • Altos costos publicitarios. • Recursos obsoletos. • Resultados financieros no favorables. • Mercado digital rentable. • Gestión ambiental. • Rotación de personal.
Oportunidades	**Amenazas**
• Necesidad del producto. • Fuerte poder adquisitivo. • Reinventar el portafolio atendiendo competentemente la nueva dinámica de los anunciantes. • Uso de recursos tecnológicos para publicar noticas de los medios de comunicación. • Incorporar audiencia en dispositivos móviles. • Directivos en busca de mayores ingresos para la empresa. • Ser el diario de mayor proyección entre la juventud.	• Competencia muy agresiva. • La nueva Ley de Comunicación Social del país. • Aranceles a la importación del papel periódico • Cambio en las necesidades y gustos de los compradores. • Nuevas tendencias de medios digitales. • Poder económico de la competencia directa. • Potencial innovación de las empresas en nacionales en el mercado.

Elaborado por: Carmen Bastidas

1.2.9 Organigrama de la empresa

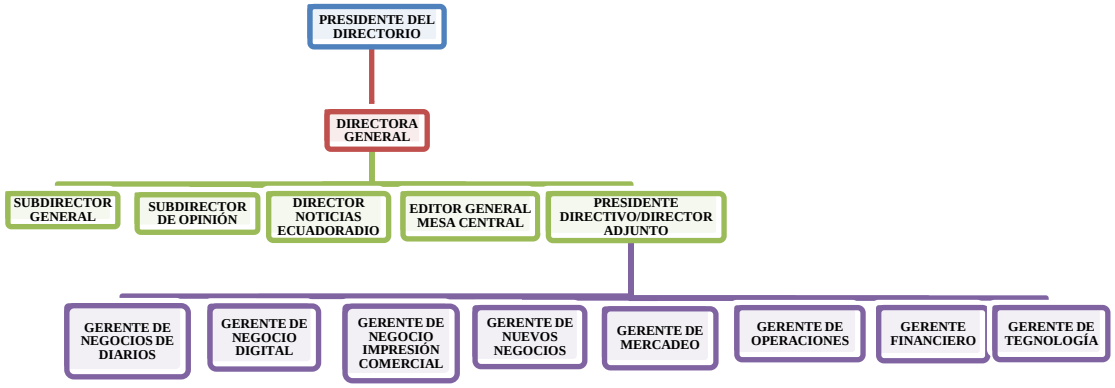


Figura 4. Organigrama de la empresa Grupo El Comercio C.A.

Elaborado por: Carmen Bastidas

1.2.10 Descripción de la gerencia y áreas

Gerencial General: Tiene como propósito dirigir, organizar y coordinar el funcionamiento y desarrollo de los procesos y actividades diarias de acuerdo con sus políticas de la organización.

Área de Redacción o RIM (Redacción Integrada Multimedia): Genera contenidos en todos los medios, marcas, productos y plataformas de Grupo El Comercio C.A. Está liderada por la mesa central, cuyas funciones principales son planificar, organizar y ejecutar estrategias de trabajo periodístico. Tiene un esquema 24/7 (24 horas/7 días de trabajo) y una producción multimedia y multiproducto. La RIM está en constante innovación para ofrecer a sus audiencias contenidos de alta calidad.

Área de Desarrollo Digital y Tecnología: Tiene como objetivos el desarrollo, puesta en marcha y operación de soluciones tecnológicas que apoyen la meta de convertir a Grupo El Comercio C.A. en la mejor empresa de medios de comunicación del país.

El aporte de los servicios informáticos tiene que estar subdividida, para así ser más específicos al momento de las comunicaciones y aplicaciones, para brindar un servicio de calidad y excelencia de la industria.

1.3 Auditoría Informática

1.3.1 Introducción a la Auditoría Informática

Con el desarrollo de las empresas se ha hecho necesario contar con la presencia de un auditor anteriormente conocido como revisor. En el caso de los auditores de sistemas de información, su trabajo ha ido de la mano al desarrollo tecnológico de su época.

La Auditoría Informática deberá comprender no sólo la evaluación de los equipos de computación, de un sistema, sino que además habrá de evaluar los sistemas de información en general.

La práctica de este tipo de auditoría ha aumentado en nuestro país durante los últimos años. La Auditoría Informática es importante en las organizaciones porque de esta manera se pueden visualizar las varias formas en que se mal utilizan los equipos de computación de una organización.

Es importante aclarar que la informática en sí misma es solamente un apoyo en la toma de decisiones de una empresa; es decir, carece de autonomía. Justamente por esa razón es importante la existencia de la Auditoría Informática para el buen funcionamiento de una compañía.

Entonces, la auditoría es un examen crítico, que se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos que se tienen establecidos en una empresa ya sea pública o privada, que no implica necesariamente la preexistencia de fallas en la entidad auditada ya que persigue el fin de evaluar y mejorar la eficiencia, eficacia y seguridad de los Sistemas de Información de un organismo.

Todo clase de compañías, en lo que tiene que ver en su desarrollo interno, necesita de los recursos de Tecnologías de la Información (TI), para asegurar un sostenido crecimiento del negocio.

Haciéndose eco de estas tendencias, Information Systems Audit and Control Association (ISACA), a través de su fundación, publicó en diciembre de 1995 el COBIT para los procesos de TI.

1.3.2 Conceptos de Auditoría y Auditoría Informática

La auditoría es una revisión metódica, periódica e intelectual de los registros que se encarga de analizar los mecanismos de control de una empresa, con el fin de evaluar si estos cumplen las metas planteadas a través de las estrategias y, de ser necesario, establecer los cambios que se deberían realizar para la consecución de los mismos.

> **Auditar** consiste en el: Conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente de acuerdo con las normas informáticas y generales existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente. (Padlocks, Auditoría de Sistema, 2013)

Informática: Es la ciencia que estudia el tratamiento automático de la información utilizando técnicas, procesos y máquinas para apoyar y potenciar su capacidad de memoria, de pensamiento y de comunicación (Castro, 2012, pág. 16)

En informática se evalúa la eficiencia y eficacia con que los procesos informáticos funcionan, para que por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

> **La Auditoría Informática:** Conjunto de procedimientos y técnicas que permiten en una entidad: evaluar, total o parcialmente, el grado en que se cumplen la

observancia de los controles internos asociados al sistema informático; determinar el grado de protección de sus activos y recursos; verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en la entidad, y para conseguir la eficacia exigida en el arco de la organización correspondiente. (Martínez Alfonso, 2012, pág. 4)

1.3.3 Auditoría en TICs (Tecnologías de la Información y Comunicación)

La auditoría en TICs es un conjunto de procesos metodológicos que permiten tener una evaluación, total o parcial, del sistema informático de una empresa, para salvaguardar sus recursos y, a la vez, comprobar si sus actividades se desarrollan conforme a la normativa informática establecida. Esto, con el fin de conseguir la eficacia exigida por la organización.

"Es muy importante recalcar que la función de la auditoria en TIC´S es prevenir desvíos, modificaciones o manipulaciones a la información, analiza el control de la función Informática, el análisis de la eficiencia de los sistemas informáticos, la verificación del cumplimiento de la normatividad general, la revisión de la gestión de los recursos materiales, humanos e informáticos, los niveles de seguridad, etc." (Castro, 2012, pág. 15)

1.3.4 Objetivos de la Auditoría Informática

El principal objetivo de la Auditoría Informática es recomendar a la administración de una empresa el cumplimiento efectivo de sus responsabilidades, facilitándoles análisis, apreciaciones, comentarios y recomendaciones con las actividades del procesamiento de la información.

Se pueden determinar, además, otros objetivos como:

- El control de la función informática.

- El análisis de la eficiencia de los sistemas informáticos.
- La verificación del cumplimiento de la normativa en este ámbito.
- La revisión de la eficaz gestión de los recursos informáticos.

La Auditoría Informática sirve para mejorar ciertas características en la empresa como:

- Eficiencia.
- Eficacia.
- Rentabilidad
- Seguridad.

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la Auditoría Informática ha promovido la creación y desarrollo de mejores prácticas como COBIT, COSO e ITIL. (Lupe, 2011, pág. 1)

1.3.5 Importancia

La Auditoría Informática ayuda a establecer con exactitud si la actividad informática se la está manejando adecuadamente, por medio de evaluaciones realizadas por personal capacitado o, a la vez, evaluaciones periódicas realizadas por el mismo personal de Informática.

Los procesos claves de las empresas que son llevados por aplicaciones informáticas, el aparecimiento de nuevas tecnologías que facilitan ciertas operaciones que deben ser contraladas en cuanto a seguridad, la automatización de sus controles, la integración de la información tanto para agilitar procesos como para tomar decisiones, entre otros, deben ser elementos que requieren de controles que son llevados por una Auditoría Informática, de ahí su importancia.

No se puede descartar a la TI como factor primordial en el éxito de las empresas. Pues es justamente el notable desarrollo de la Auditoría Informática lo que ha permitido a las compañías dar importancia a la necesidad de protección de su actividad informática en todas sus áreas de trabajo.

1.3.6 Tipos de Auditoría Informática

- **Auditoría interna**: es el examen crítico, sistemático y detallado de un sistema de información, realizado por un profesional con vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir informes y formular sugerencias para el mejoramiento de la misma. Estos informes son de circulación interna y no tienen trascendencia a los terceros pues no se producen bajo la figura de Fe Pública. (Lupe, 2011, pág. 2)
- **Auditoría externa**: Examina y evalúa cualquiera de los sistemas de información de una organización y emite una opinión independiente sobre los mismos, pero las empresas generalmente requieren de la evaluación de sus sistemas de información en forma independiente para otorgarle validez ante los usuarios del producto de este, por lo cual tradicionalmente se ha asociado el término auditoría externa a auditoría de estados. (Lupe, 2011, pág. 1)

1.3.7 Estructura del proceso de Auditoría Informática;

La aplicación de una auditoría se fundamenta en procesos aplicables a determinadas circunstancias; es a esto lo que se denomina procedimientos de auditoría en informática. Para lograr esto se realiza la recolección y evaluación de evidencias que debe seguir un orden como son:

- Planificación de la Auditoria Informática.
- Ejecución de la Auditoria Informática.
- Finalización de la Auditoria Informática. (Castro, 2012, pág. 20)

1.3.7.1 Planificación de la Auditoría Informática

Este inicia con una fase de planeación donde se encuentran involucrados los departamentos a ser auditados, para identificar los recursos necesarios que permitirán que se lleve a cabo, planteando objetivos como son:

- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.
- Evaluación del proceso de datos.

Obteniendo el conocimiento inicial de la entidad. se establecerán metas, programas de trabajo de auditoría, personal que intervendrá en el proyecto, presupuesto financiero, y las fechas y la manera como se presentarán los informes de las actividades de cumplimiento del proyecto. (Castro, 2012, pág. 21)

1.3.7.2 Ejecución de la auditoría

La ejecución de la Auditoría Informática constituye la recopilación de la mayor cantidad de información necesaria, como son documentos y evidencias que permitan al auditor fundamentar sus comentarios, sugerencias y recomendaciones, con respecto al manejo y administración de TI.

Para la recolección de información se pueden aplicar las siguientes técnicas:

- Entrevistas.
- Encuestas.
- Cuestionarios.
- Análisis de la información documentada.
- Revisión y análisis de estándares.

Toda la información recabada entra luego en un proceso de análisis, en donde debe ser clasificada de manera que permita ubicarla fácilmente y además permita, luego del análisis respectivo, justificar de manera correcta las recomendaciones.

La evidencia se clasifica de la siguiente manera:

- Evidencia documental.
- Evidencia física.
- Evidencia analítica.
- Evidencia testimonial. (Castro, 2012, pág. 21)

1.3.8 Finalización de la Auditoría Informática

El resultado de la Auditoría Informática se materializa en un informe de conclusiones y recomendaciones que se debe redactar y entregar a la administración de la organización para su evaluación y análisis, por lo que antes de la emisión del informe final se debe realizar varios borradores, para descubrir fallos en la evaluación de auditoría debido a la incorrecta comprensión de la organización por parte del auditor. (Castro, 2012, pág. 21)

1.3.9 Fases de la Auditoría Informática

Kuna, en su Tesis de Magíster: "Asistente para la realización de Auditoría de Sistemas en Organismos Públicos o Privados", enuncia una metodología de desarrollo de AI, que coincide con varias propuestas de diferentes autores. Se contemplan las siguientes fases:

Fase 1. Identificar el alcance y los objetivos de la Auditoría Informática

Esta primera etapa sirve para definir los términos y el contexto en los cuales se realizará la auditoría. Para lograr el éxito es indispensable que exista un acuerdo claro y exacto entre el auditor y las autoridades de la organización.

Fases 2. Realizar el estudio inicial del entorno a auditar

"En esta fase es necesario examinar las funciones y actividades generales de la organización a auditar y en particular de las relacionadas con las tecnologías de la información. Se debe definir el organigrama, los departamentos, las relaciones funcionales y jerárquicas entre las distintas áreas de la organización, el flujo de información, el número de puestos de trabajo y personas por puesto de trabajo, la estructura organizativa del Departamento de Informática, características de hardware y software, las metodologías de desarrollo y mantenimiento de aplicaciones, y aspectos relacionados con la seguridad." (Kuna, 2006, pág. 23)

Fase 3. Determinación de los recursos necesarios para realizar la Auditoría Informática

Después de realizar el estudio preliminar, se debe determinar herramientas e instrumentos necesarios para implementar el plan de auditoría. (Kuna, 2006, pág. 24)

Fase 4. Elaborar el plan de trabajo

En esta fase se define el calendario de actividades a realizar, formalizando el mismo para la aprobación por parte de las autoridades. Ver tabla 2. (Kuna, 2006, pág. 25)

Fase 5. Realizar las actividades de auditoría

Es el momento donde se efectivizan las actividades planificadas en la fase anterior, aplicando distintas técnicas y utilizando herramientas que garanticen el cumplimiento de los objetivos planteados. (Kuna, 2006, pág. 25)

Fase 6. Realizar el informe final

"La elaboración del informe final es la única referencia constatable de toda auditoría, y el exponente de su calidad". (Kuna, 2006, pág. 25)

Fase 7. Carta de presentación

Es la última etapa de auditoría y consta de un resumen del contenido del informe final, dirigido a las autoridas de la organización. (Kuna, 2006, pág. 27)

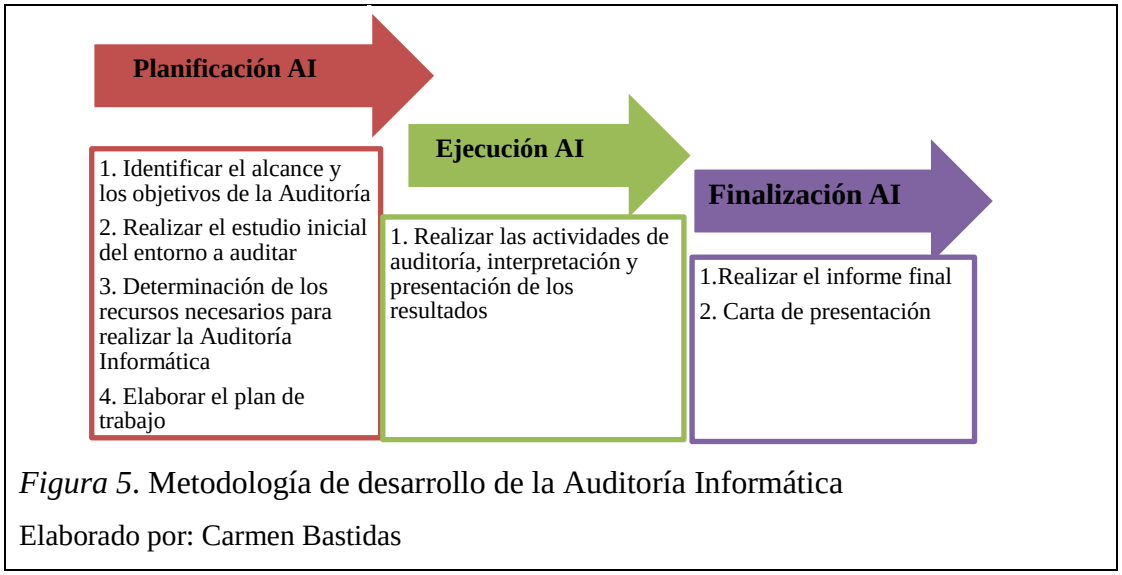


Figura 5. Metodología de desarrollo de la Auditoría Informática

Elaborado por: Carmen Bastidas

Tabla 2

Calendario de actividades a realizar en la auditoría

Fases de la auditoría del Grupo El Comercio C.A.	**Semanas durante la auditoría**															
Planificación	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Identificar el alcance y los objetivos de la auditoría																
Realizar el estudio inicial del entorno a auditar																
Determinación de los recursos necesarios para realizar la Auditoría Informática																
Elaborar el plan de trabajo																
Ejecución																
Realizar las actividades de auditoría, interpretación y presentación de los resultados																
Finalización																
Realizar el informe final																
Carta de presentación																

Elaborado por: Carmen Bastidas

1.3.10 Normas, técnicas, estándares y procedimientos de la Auditoría Informática

Las normas de auditoría tienen que ver con la calidad, relacionada a las cualidades del auditor, así como su labor responsable y la información que brinde como fruto de esa labor.

Las técnicas son los métodos prácticos de investigación y prueba que utiliza el auditor para obtener la evidencia necesaria que fundamente sus opiniones y conclusiones.

Los procedimientos son el conjunto de técnicas de investigación aplicables a un grupo de hechos o circunstancias, para fundamentar la opinión del auditor.

1.3.11 Organizaciones y Normas de AI (Auditoría Informática) más relevantes.

Actualmente el Ecuador cuenta con un marco regulatorio y normativo reducido en materia informática, es por ello que se estudiarán las normas y organizaciones internacionales más relevantes en este ámbito.

Las organizaciones más importantes son: Institute of Internal Auditors (IIA), e Information System Audit and Control Association (ISACA) que han desarrollado normas y estándares con el fin de establecer políticas y lineamientos que garanticen el proceso de auditoría. Algunos de los estándares más conocidos son:

Tabla 3

Cuadro comparativo entre COBIT, ITIL y la ISO 27000

ÁREA	COBIT	ITIL	ISO 27000
Alcance	De las actividades de IT (seguridad, control, servicios y riesgo)	Muy centrado en la administración de servicios	Cubre todo lo referente a la entrega de servicios de TI
Objetivo general	Establecer controles internos para asegurar buenas prácticas de gestión de IY y un gobierno de IT exitoso.	Dar soporte a los procesos del negocio desde una perspectiva de gestión de servicios.	Definir los requerimientos necesarios para realizar una entrega de servicios de TI alineados con las necesidades del negocio.
Funciones	Mapeo de procesos IT	Mapeo de la Gestión de Niveles de Servicio de IT.	Marco de referencia de seguridad de la información.
Áreas	4 Procesos y 34 Dominios	9 Procesos	10 Dominios
¿Para qué se implementa?	Auditoría de Sistemas de Información	Gestión de Niveles de Servicio	Cumplimiento del estándar de seguridad
¿Quiénes lo evalúan?	Compañías de contabilidad, Compañías de consultoría en TI	Compañías de consultoría en TI	Compañías de consultoría en TI, Empresas de seguridad, Consultores de seguridad en redes

Elaborado por: Carmen Bastidas

1.4 Generalidades del modelo COBIT

1.4.1 Análisis del estándar COBIT

COBIT es uno de los estándares más utilizados actualmente, como base en la realización de una metodología de control interno en el ambiente de tecnología informática. COBIT es un marco de referencia y se fundamenta en los objetivos de

control existentes de la ISACF, y se encuentra alineado con otros estándares de control y auditoría como COSO, IFAC, IIA, ISACA, AICPA.

Misión de COBIT: la misión COBIT es investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento (IT Governance Institute, 2007, pág. 9)

1.4.2 Orientado a negocios

El modelo de COBIT está orientado a negocios, ya que se encuentra diseñado para ser una guía para la gerencia, propietarios de los procesos de negocio, los proveedores de servicios, usuarios y auditores de TI. Además es el enfoque de control en TI que se lleva a cabo visualizando la información necesaria para dar soporte a los procesos del negocio. Siendo la información el resultado de la aplicación combinada de recursos relacionados con la tecnología de la información, que deben ser administrados por procesos TI. (IT Governance Institute, 2007, págs. 9-12)

El marco de trabajo de COBIT ofrece herramientas para garantizar la alineación de la administración de TI con los requerimientos del negocio, basados en los principios básicos del COBIT. En donde los requerimientos de información del negocio deben adaptarse a ciertos criterios de información, para que la misma permita cumplir con los objetivos de la organización, los cuales son:

- **Efectividad:** la información relevante y pertinente al proceso del negocio existe y es entregada a tiempo, correcta, consistente y utilizable.
- **Eficiencia:** es la optimización (más económica y productiva) de los recursos que se utilizan para la provisión de la información.
- **Confidencialidad:** es relativo a la protección de información, así como a su validez de acuerdo con las expectativas del negocio.

- **Integridad:** se refiere a lo exacto y completo de la información, así como a su validez de acuerdo con las expectativas del negocio.

- **Disponibilidad:** accesibilidad a la información para los procesos del negocio en el presente y en el futuro, también salvaguardar los recursos y capacidades asociadas a los mismos.

- **Cumplimiento:** son las leyes, regulaciones, acuerdos contractuales a los que el proceso del negocio está sujeto.

- **Confiabilidad de la información:** proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con las responsabilidades de los reportes financieros.

Una vez que las metas del negocio se encuentran alineadas y han sido definidas, requieren ser monitoreadas para garantizar que la entrega cumpla con las expectativas del negocio.

Los recursos de TI son:

- **Datos:** todos los objetos de información interna y externa, estructurada o no, gráficas, sonidos, etc.

- **Aplicaciones:** los sistemas de información, que integran procedimientos manuales y sistematizados.

  Tecnología: tiene que ver con sistemas operativos, administración de redes, de bases de datos, con hardware y software, multimedia, entre otros.

- **Instalaciones:** son recursos necesarios para alojar y dar soporte a los sistemas de información.

- **Talento humano:** cualidades del personal relacionadas con la facilidad para planificar, adquirir, apoyar y vigilar el buen funcionamiento de los sistemas de información.

Se debe gestionar todos los recursos de TI, mediante un conjunto de procesos agrupados, para lograr metas de TI que proporcionen la información que el negocio necesita para alcanzar sus objetivos. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT.

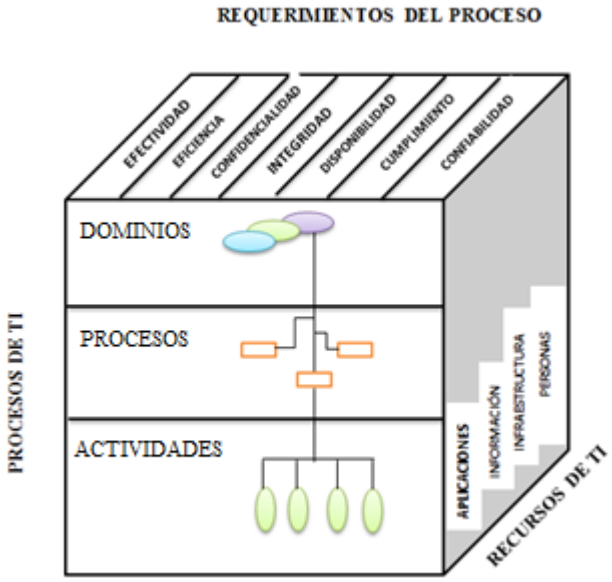


Figura 6. El cubo de COBIT

Fuente: IT Governance Institute, 2007, pág. 25

Elaborado por: Carmen Bastidas

1.4.3 Orientado a procesos

Se pueden diferenciar tres niveles de actividades en un proceso de TI:

- **El nivel superior de agrupación:** son los dominios que constituyen los procesos agrupados, los dominios en una estructura organizacional se denominan dominios de responsabilidad y se alinean con el ciclo de vida o administrativo de los proceso TI.
- **En el nivel intermedio:** se encuentran los procesos, que son un conjunto de varias tareas y actividades.
- **En el nivel bajo:** se hallan las actividades y tareas necesarias para alcanzar un resultado medible, es decir, son las actividades más discretas.

1.4.4 Dominios

COBIT presenta 34 objetivos generales, uno para cada uno de los procesos de las TI; estos procesos están agrupados en cuatro dominios, como lo muestra la figura 7.

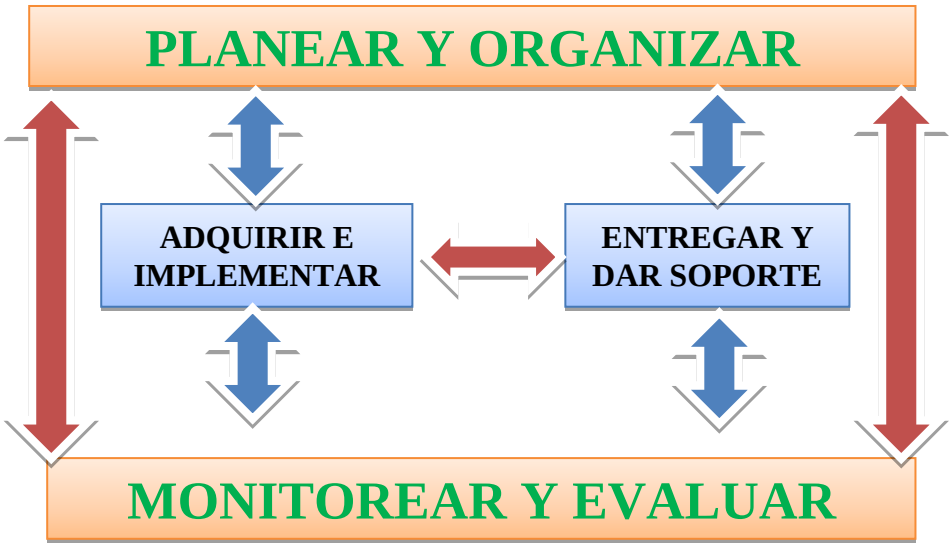


Figura 7. Los cuatro dominios de COBIT
Fuente: IT Governance Institute, 2007, pág. 12
Elaborado por: Carmen Bastidas

1.4.4.1 Planear y organizar (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrativa desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- **PO1** Definir una plan estratégico de tecnología de la información.
- **PO2** Definir la arquitectura de información.

- **PO3** Determinar la dirección tecnológica.
- **PO4** Definir la organización y de las relaciones de TI.
- **PO5** Manejar la inversión en Tecnología de la Información.
- **PO6** Comunicar la dirección y aspiraciones de la gerencia.
- **PO7** Administrar recursos humanos.
- **PO8** Asegurar el cumplimiento de requerimientos externos.
- **PO9** Evaluar riesgos.
- **PO10** Administrar proyectos.
- **PO11** Administrar calidad.

1.4.4.2 Adquirir e implementar (AI).

Para desempeñar la estrategia de TI es necesario que sus soluciones estén claramente identificadas y desarrolladas, así como también, la incorporación en los procesos de la empresa y sus objetivos. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- **AI1** Identificar soluciones.
- **AI2** Adquirir y mantener software de aplicación.
- **AI3** Adquirir y mantener arquitectura de tecnología.
- **AI4** Desarrollar y mantener procedimientos relacionados con TI.
- **AI5** Instalar y acreditar sistemas.
- **AI6** Administrar cambios.

1.4.4.3 Entregar y dar soporte (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- **DS1** Definir niveles de servicio.
- **DS2** Administrar servicios prestados por terceros.
- **DS3** Administrar desempeño y capacidad.
- **DS4** Asegurar servicio continuo.
- **DS5** Garantizar la seguridad de sistemas.
- **DS6** Identificar y asignar costos.
- **DS7** Educar y entrenar a los usuarios.
- **DS8** Apoyar y asistir a los clientes de TI.
- **DS9** Administrar la configuración.
- **DS10** Administrar problemas e incidentes.
- **DS11** Administrar datos.
- **DS12** Administrar instalaciones.
- **DS13** Administrar operaciones.

1.4.4.4 Monitorear y evaluar (ME).

Es importante que los procesos de TI se evalúen de forma constante, en lo que tiene que ver con su calidad y ejecución, en base a las exigencias de control. Este dominio

abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- **M1** Monitorear los procesos.
- **M2** Evaluar lo adecuado del control interno.
- **M3** Obtener aseguramiento independiente.
- **M4** Proporcionar auditoría independiente.

En síntesis, lo que se requiere es que los recursos de TI sean regidos por procesos agrupados sistemáticamente, para poder facilitar la entrega de información a las autoridades de la empresa para que continúen en el alcance de sus objetivos, tal como se muestra en la figura 8.

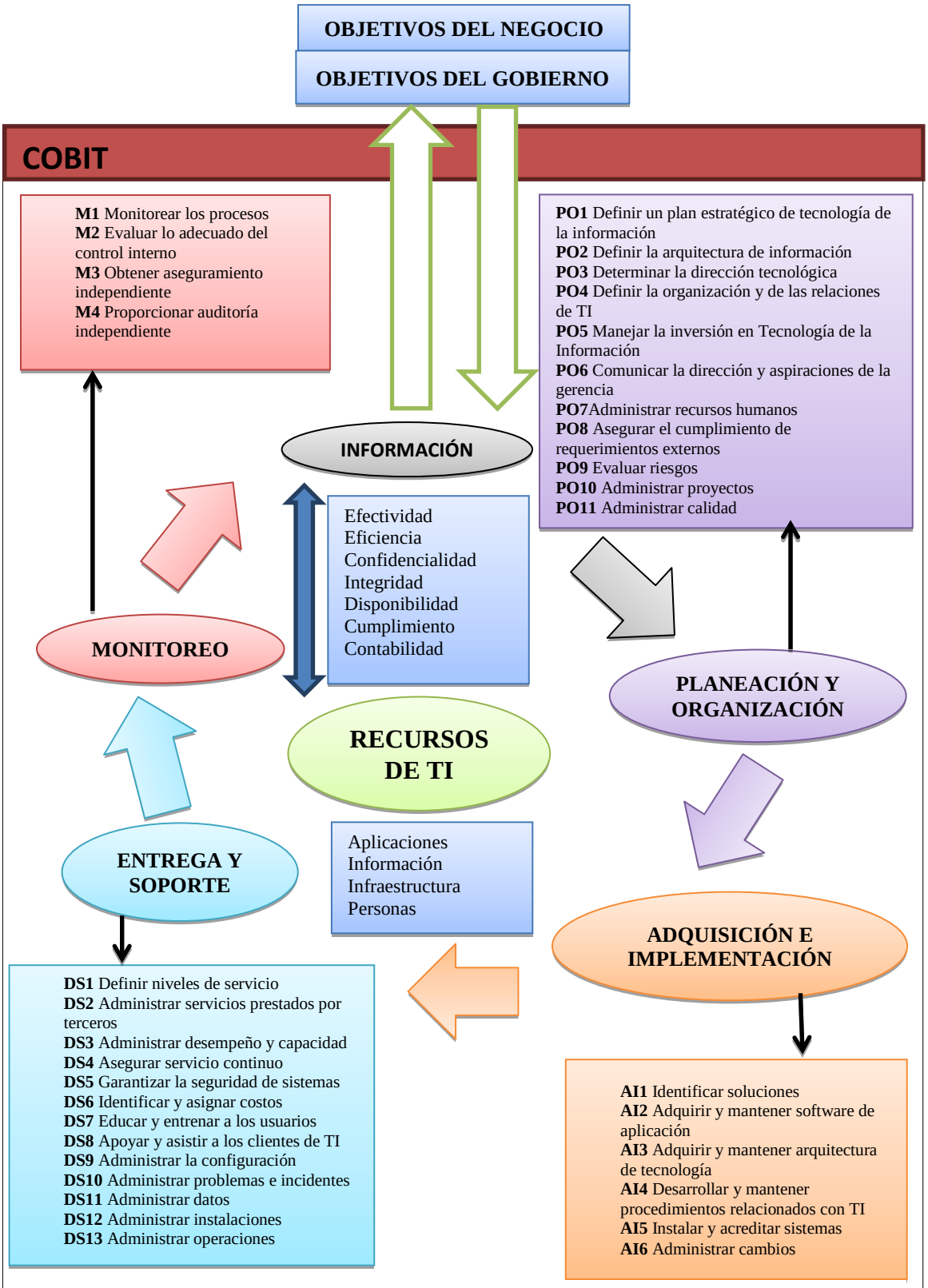


Figura 8. Marco de trabajo completo de COBIT
Fuente: IT Governance Institute, 2007, pág. 30
Elaborado por: Carmen Bastidas

1.4.5 Objetivos de control

Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT están directamente relacionadas con los requerimientos elementales para una verificación exacta de cada proceso TI. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados.

Los objetivos de control detallados se identifican por dos caracteres que representan el dominio (PO, AI, DS y ME) más un número de proceso y un número de objetivo de control.

Modelos de madurez

Estos consisten en la elaboración de un método de puntaje, con el fin de que una empresa determinada pueda autoevaluarse desde la categoría inexistente hasta la optimizada (de 0 a 5). Este método ha sido derivado del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software. Contra estos niveles, desarrollados para cada uno de los 34 procesos de TI de COBIT, la administración puede mapear o cruzar:

- El estado actual de la organización -dónde está la organización actualmente.
- El estado actual de la industria (la mejor de su clase en) -la comparación.
- El estado actual de los estándares internacionales -comparación adicional.
- La estrategia de la organización para mejoramiento -dónde quiere estar la organización.

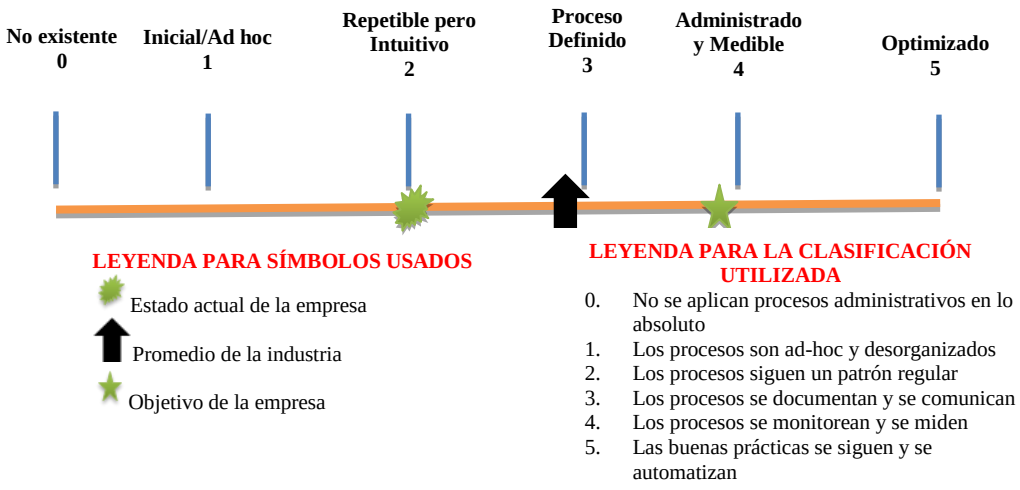


Figura 9. Representación gráfica de los modelos de madurez

Fuente: IT Governance Institute, 2007, pág. 22

Elaborado por: Carmen Bastidas

0 Inexistente: carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1 Inicial: existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándares; en su lugar existen enfoques ad-hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible: se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido: los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados, pero formalizan las prácticas existentes.

4 Administrado: Es factible vigilar y evaluar que los procesos se cumplan a cabalidad; de no ser así hay que tomar medidas reales y prácticas. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado: La obtención de resultados óptimos de manera continua tiene que ver con un sobresaliente nivel del cumplimiento de los procesos y en un ejemplo de madurez con otras organizaciones. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar localidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

En resumen, los modelos de madurez brindan un perfil genérico de las etapas a través de las cuales evolucionan las empresas para la administración y el control de los procesos de TI; este perfil es:

- Un conjunto de requerimientos y los aspectos que los hacen posible en los distintos niveles de madurez.
- Una escala donde la diferencia se puede medir de forma sencilla.
- Una escala que se presta a sí misma para una comparación práctica.
- La base para establecer el estado actual y el estado deseado.
- Soporte para un análisis de brechas para determinar qué se requiere hacer para alcanzar el nivel seleccionado.
- Tomado en conjunto, una vista de cómo se administra la TI en la empresa. (IT Governance Institute, 2007, págs. 18-20)

CAPÍTULO 2

APLICACIÓN DE LA AUDITORÍA INFORMÁTICA

2.1 Áreas a auditar

La auditoría realizada será en las áreas de Redacción y de Tecnología de Grupo El Comercio C.A.

2.1.1 Situación actual de las áreas de Redacción y de Tecnología

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR	GRUPO EL COMERCIO
Área de Redacción	**Área de Desarrollo y Tecnología**
	

Figura 10. Situación actual de las áreas de Redacción y de Tecnología
Fuentes: http://somos/areas/desarrollo-y-tecnologia.html ,
http://somos/areas/rim.html

2.1.2 Objetivos del Departamento de Redacción, RIM

- Seguir creciendo.
- Consolidar su liderazgo en los medios impresos y alcanzarlo en el mundo digital y en la radio.
- Desarrollar otras plataformas y captar nuevas audiencias. Para conseguir este objetivo, el grupo se basaría en su independencia y credibilidad para atender a

las audiencias según los hábitos de consumo de estas: a todas horas, en todas partes y a través de múltiples plataformas.

2.2 Organigrama del departamento

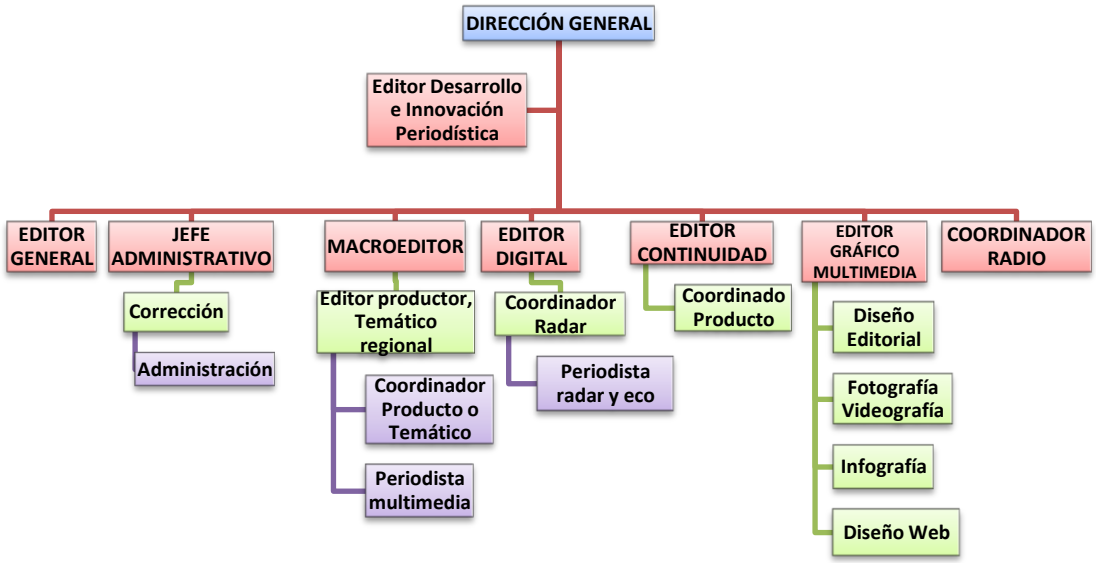


Figura 11. Organigrama del Departamento de Redacción

Elaborado por: Carmen Bastidas

2.2.1 Objetivos del Departamento de Tecnología

- Planificar, implementar y mantener la infraestructura tecnológica de la empresa. Hardware y software y comunicaciones, de tal forma que pueda estar disponible para los usuarios aplicando estándares de eficiencia y calidad.

- Construir e implementar las nuevas aplicaciones financieras, administrativas, comerciales y digitales-multimedia de acuerdo con el plan estratégico de la empresa.

- Ejecutar las mejores prácticas, técnicas y de procesos, para la entrega de campañas publicitarias.

2.3 Organigrama del departamento

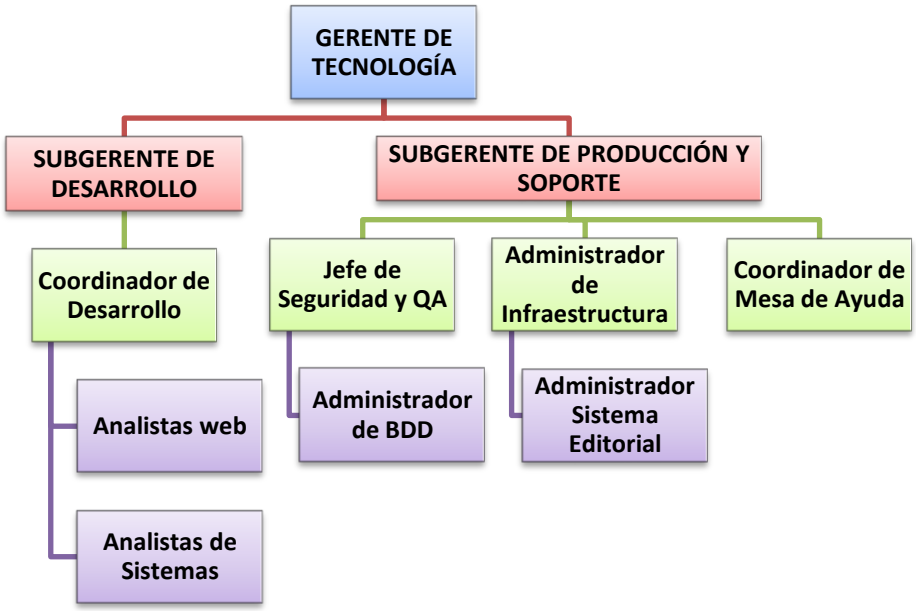


Figura 12. Organigrama del Departamento de Tecnología

Elaborado por: Carmen Bastidas

2.4 Selección de los procesos a ser auditados

Para tener un criterio del medio de trabajo se sigue una metodología de auditoria general, y los criterios del modelo de COBIT que dan un marco de referencia y de trabajo estandarizado, que involucren documentos con temas clasificados a través de dominios, procesos y actividades.

2.4.1 Dominio planear y organizar (PO)

PO1 Definir un plan estratégico

La planeación estratégica de TI es necesaria para evaluar el desempeño actual y asegurar el valor óptimo de los proyectos y portafolio de servicios de acorde con las necesidades actuales y futuras del negocio, manejando adecuadamente las tecnologías de la información para así alcanzar las metas del negocio.

Objetivos de control

- Disponer una valoración de los procesos de la empresa, incluso en el área financiera, considerando los riesgos de incumplimiento que no permitan lograr las metas trazadas.
- Integrar las estrategias del negocio y de TI, relacionando de manera clara las metas de la empresa y las metas de TI, reconociendo las oportunidades, así como las limitaciones, educando a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro.
- Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio.
- Incluir en el plan estratégico el presupuesto de la inversión operativa, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición y los requerimientos legales y regulatorios.
- Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico.
- Administrar el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos asignando recursos y financiamiento.

PO2 Definir la arquitectura de la información

Se debe definir los sistemas apropiados para optimizar el uso de información. Esto incluye el desarrollo de un diccionario corporativo de datos que contenga el esquema de clasificación de datos y los niveles de seguridad. Este proceso de TI es necesario para establecer el control de la información compartida a lo largo de las aplicaciones y de las entidades.

Objetivos de control

- Establecer y mantener un modelo de información empresarial basado en qué tan crítica y sensible es la información (esto es: pública, confidencial, secreta). Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección.
- Definir e implementar procedimientos para garantizar la integridad y consistencia de los datos, fomentando un entendimiento común de datos entre los usuarios de TI y del negocio.

PO3 Determinar la dirección tecnológica

La función de servicios de información debe determinar la dirección tecnológica para dar soporte al negocio. Para esto es necesario elaborar un plan de recursos tecnológicos que ayuden a obtener resultados idóneos a los cambios en el ambiente empresarial.

Objetivos de control

- Crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos.
- Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, es decir, sistemas aplicativos estándares y bien integrados y estables.

PO6 Comunicar las aspiraciones y la dirección de la gerencia

La dirección debe elaborar un marco de control empresarial de TI, definir y comunicar las políticas asegurándose que se implanten y se comuniquen a todo el

personal relevante y a todos los usuarios de la organización, así como de la conciencia y el entendimiento de los objetivos y la dirección del negocio.

Objetivos de control

- Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa.
- Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial y a un conjunto de políticas que apoyen la estrategia de TI.
- Asegurar que se instaure y se comunique a todo el personal relevante las políticas de TI, y se refuercen, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales.

2.4.2 Dominio adquirir e implementar (AI)

AI1 Identificar soluciones automatizadas

La necesidad de una nueva aplicación o función requiere de un análisis para garantizar que los requisitos del negocio se satisfacen en un enfoque efectivo y eficiente. Este proceso realiza una revisión de factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio y concluye con una decisión final de desarrollar o comprar. Este procedimiento ayuda a que las empresas logren minimizar el gasto de adquisición e implementación de soluciones, así como también cumplir con más facilidad los objetivos organizacionales.

Objetivos de control

- Definir y mantener los requerimientos técnicos y funcionales requeridos para lograr los resultados esperados de los programas de inversión en TI.
- Realizar un reporte de riesgo, identificando, documentando y analizando los riesgos asociados a los requerimientos del negocio y diseño de soluciones,

como parte de los procesos organizacionales para el desarrollo de los requerimientos.

- Verificar que el proceso requiere al patrocinador del negocio para aprobar y autorizar la decisión final con respecto a la elección de la solución y al enfoque de adquisición, tomando la decisión de compra vs. desarrollo.

AI2 Adquirir y mantener software aplicativo

Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y configuración en sí de acuerdo con los estándares.

Objetivos de control

- Adquirir y mantener aplicaciones que satisfagan en forma rentable los requerimientos definidos para el negocio.
- Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación, los requerimientos de calidad y estándares de aprobación. Asegurar que todos los aspectos legales y contractuales se edifican y direccionan para el software aplicativo.
- Ejecutar un plan de aseguramiento de calidad de software.
- Desarrollar una estrategia y un plan para el mantenimiento de aplicaciones de software.

AI3 Adquirir y mantener infraestructura tecnológica

Ninguna empresa debe descuidar la adquisición, correcta utilización y actualización de toda la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias

tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.

Objetivos de control

- Desarrollar un plan para la compra, implementación y mantenimiento constantes de la infraestructura tecnológica, que esté de acuerdo con las necesidades funcionales y técnicas del negocio, y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología.
- Monitorear y evaluar los recursos de infraestructura.
- Disponer de un entorno adecuado para la realización de pruebas que ayuden a establecer la eficiencia y la efectividad de las aplicaciones e infraestructura.
  Hay que considerar la funcionalidad, la configuración de hardware y software, migración entre ambientes, control de las versiones, datos y herramientas de prueba y seguridad.

AI4 Facilitar la operación y el uso

Debe existir fácil acceso al conocimiento de las actualizaciones de los sistemas, a través de manuales y documentos acorde a los usuarios y para TI. Sólo así se puede garantizar un uso óptimo de los sistemas informáticos.

Objetivos de control

- Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos.
- Transferir el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos y ejercer la responsabilidad por la entrega y

calidad del servicio, del control interno y de los procesos administrativos de la aplicación.

- Transmitir a los usuarios la capacidad y la habilidad de una correcta utilización del sistema de aplicación, como un recurso de apoyo a los procesos empresariales.

- Compartir con el personal técnico y operativo, las competencias y destrezas para salvaguardar la infraestructura informática de manera óptima, con relación a los niveles de servicio determinados.

2.4.3 Dominio entregar y dar soporte (DS)

DS4 Garantizar la continuidad del servicio

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, ya que minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI.

Objetivos de control

- Desarrollar un marco de trabajo de continuidad de TI con base al marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos claves del negocio.

- Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, sin dejar de lado el recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio.

- Probar el plan de continuidad de TI de forma regular, para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable.

- Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de una manera continua los requerimientos del negocio.

- Asegurarse que todos las partes involucradas en el plan de continuidad TI reciban capacitaciones de forma regular respecto a los procesos y sus roles y responsabilidades en caso de desastres.

DS5 Garantizar la seguridad de los sistemas

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este aspecto involucra tener presente en todo momento las funciones y deberes de seguridad, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad.

Objetivos de control

- Administrar la seguridad en TI, con el máximo grado de eficiencia, de tal manera que la administración de la seguridad esté acorde con las demandas de la empresa y, además, tomando en cuenta la cultura de seguridad juntamente con la infraestructura de TI. Asegurar que el plan está implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware.

- Garantizar que todos los usuarios internos, externos y temporales estén identificados de manera única, de tal manera que se utilicen libremente mecanismos de autenticación.

- Avalar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.

- Poner medidas preventivas, detectivas y correctivas en toda la organización, para proteger los sistemas de información y a la tecnologías contra malware (virus, gusanos, spyware, correo basura…).

- Usar técnicas de seguridad y procedimientos de administración asociados para autorizar acceso y controlar los flujos de información desde y hacia las redes.

DS9 Administrar la configuración

Proteger todas las configuraciones de hardware y software a través de un almacenamiento de información completo y seguro. Esto ayuda a tener un registro de los activos de TI, actualizado y preciso.

Objetivos de control

- Establecer una herramienta de soporte y un repositorio central que contenga toda la información relevante sobre los elementos de configuración. Monitorear y grabar todos los activos y los cambios a los activos.

- Verificar constantemente los datos de configuración, para garantizar la integridad de la información histórica y actual.

- Revisar periódicamente el software instalado para identificar si es licenciado o no. Siendo medido con porcentajes de licencias registradas en el repositorio.

DS10 Administración de programas

Una efectiva administración de problemas requiere la identificación y clasificación de estos, el análisis de las causas desde su raíz y la búsqueda de soluciones. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario.

Objetivos de control

- Implementar procesos para reportar y clasificar problemas de acuerdo con la categoría, impacto, urgencia y prioridad, identificados como parte de la administración de incidentes.

- Identificar soluciones sostenibles indicando la causa raíz, que permita obtener reportes regulares sobre el progreso en la resolución de problemas. La administración debe monitorear el continuo impacto de los problemas conocidos en los servicios a los usuarios. En caso de que el impacto se vuelva severo se debe escalar el problema, tal vez a través de un comité determinado.

- Disponer de un procedimiento para cerrar registros de problemas después de confirmar la eliminación exitosa del error.

- Monitorear cuánto esfuerzo se aplica para minimizar los problemas.

DS11 Administración de datos

Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio cuando se requiera.

Objetivos de control

- Comprobar que toda la información a ser procesada esté completa. Esto garantizará que los resultados estén listos a tiempo y de conformidad con los requerimientos de la organización.

- Definir e implementar procedimientos para mantener un inventario de medios almacenados, para garantizar la disponibilidad de la información cuando se requiera.

- Determinar los métodos de almacenamiento y resguardo de datos, para garantizar que la información sensible y el software no se pierda, aun cuando se elimine o transfiera información, así como para respaldo y recuperación de los sistemas con los requerimientos del negocio de forma eficiente, ya que de tal manera se asegura la usabilidad, integridad y el plan de continuidad de la información.

DS12 Administración del ambiente físico

La administración del equipo de cómputo y del personal requiere de instalaciones bien diseñadas y bien administradas para proteger los activos y la información, minimizando las interrupciones del negocio.

Objetivos de control

- Definir y seleccionar los centros de datos físicos de tal manera que la estrategia de tecnología pueda soportar la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.
- Restringir el acceso al ambiente físico a aquellos que no requieren el acceso.
- Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.

DS13 Administración de operaciones

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una

administración efectiva, ya que ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.

Objetivos de control

- Definir, implementar y mantener procedimientos estándar para operaciones de TI.
- Organizar la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el desempeño y la utilización para cumplir con los requerimientos del negocio.
- Garantizar que el personal de operaciones debe cubrir los procesos de transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos de escalamiento y reporte sobre las responsabilidades actuales.
- Definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados.
- Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

2.4.4 Dominio monitorear y evaluar (ME)

ME1 Monitorear y evaluar el desempeño de TI

Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas.

Objetivos de control

- Establecer un marco de trabajo de monitoreo general, la metodología y el proceso a seguir para medir la solución y la entrega de servicios de TI, y monitorear la contribución de TI al negocio.
- Asegurar que el monitoreo constante facilite una visión clara, es decir, desde todos los ángulos, del desempeño de TI; es necesario que este monitoreo esté adaptado al de la empresa en general.
- Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial.
- Tomar acciones en caso de que el resultado del monitoreo afectase al desempeño de la empresa.

2.5 Ejecución de la auditoría

En la tabla 4 se muestran los objetivos de control escogidos para realizar la auditoría y su impacto a los criterios de información y recursos de TI.

Tabla 4

Impacto de los objetivos de control COBIT sobre los recursos y criterios TI

OBJETIVOS DE CONTROL COBIT		Recursos TI del COBIT				Criterios de información del COBIT						
	Planear y organizar (PO)	**Aplicaciones**	**Información**	**Infraestructura**	**Personal**	**Efectividad**	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**
PO1	Definir un plan estratégico	**X**	**X**	**X**	**X**	**P**	**S**					
PO2	Definir la arquitectura de la información	**X**	**X**			**S**	**P**	**S**	**P**			
PO3	Determinar la dirección tecnológica	**X**		**X**		**P**	**P**					
PO6	Comunicar las aspiraciones y la dirección de la gerencia					**P**					**S**	
	Adquirir e implementar (AI)											
AI1	Identificar soluciones automatizadas	**X**		**X**		**P**	**S**					
AI2	Adquirir y mantener software aplicativo	**X**				**P**	**P**		**S**			**S**
AI3	Adquirir y mantener infraestructura tecnológica			**X**		**S**	**P**		**S**	**S**		
AI4	Facilitar la operación y el uso	**X**		**X**	**X**	**P**	**P**		**S**	**S**	**S**	**S**
	Dominio entregar y dar soporte (DS)											
DS4	Garantizar la continuidad del servicio	**X**	**X**	**X**	**X**	**P**	**S**			**P**		
DS5	Garantizar la Seguridad de los sistemas	**X**	**X**	**X**	**X**			**P**	**P**	**S**	**S**	**S**
DS9	Administrar la configuración	**X**	**X**	**X**		**P**	**S**			**S**		**S**
DS10	Administración de programas	**X**	**X**	**X**	**X**	**P**	**P**			**S**		
DS11	Administración de datos		**X**						**P**			**P**
DS12	Administración de ambiente físico			**X**					**P**	**P**		
DS13	Administración de operaciones	**X**	**X**	**X**	**X**	**P**	**P**		**S**	**S**		
	Monitorear y evaluar (ME)											
ME1	Monitorear y evaluar el desempeño de TI	**X**	**X**	**X**	**X**	**P**	**P**	**S**	**S**	**S**	**S**	**S**

Elaborado por: Carmen Bastidas

Dónde:

(X) Significa que ese objetivo de control tiene impacto sobre el recurso.

( ) No tiene impacto.

(P) Es primario o impacto de forma directa sobre el criterio de información.

(S) Es secundario o impacto de forma indirecta sobre el criterio de información.
Para obtener los porcentajes de los criterios de información se asigna un valor al grado de impacto primario, secundario y blanco.

Para el respectivo análisis de resultados se toma como referencia el cuadro de interpretación de impacto según COSO en cuanto al nivel de riesgo:

Tabla 5

Cuadro de Interpretación de impacto

CALIFICACIÓN	GRADO DE CONFIANZA	NIVEL DE RIESGO
15% AL 50%	Bajo	Alto
51% AL 75%	Moderado	Moderado
76% AL 95 %	Alto	Bajo

Fuente: Sponsoring Organizations of the Treadway (COSO)

Elaborado por: Carmen Bastidas

Tomando en cuenta la propuesta de COSO, se ha generado una tabla de ponderaciones (tabla 6) mediante la cual se propone asignar un valor numérico al impacto de los criterios de información por cada proceso, para esto se ha determinado tomar el valor promedio de cada uno los rangos.

Tabla 6

Cuadro de promedios de impacto

NIVEL DE RIESGO	CALIFICACIÓN	GRADO DE CONFIANZA
Alto	32%	Bajo
Moderado	63%	Moderado
Bajo	86%	Alto

Fuente: Sponsoring Organizations of the Treadway (COSO),

Elaborado por: Carmen Bastidas

A continuación se colocarán los valores obtenidos en los criterios de información que establece COBIT, dentro de cada uno de los procesos, para el grado de impacto primario se asigna el 86%, cuyo impacto es alto pero su nivel de riesgo es bajo; para el grado secundario se asigna el 63% cuyo impacto y nivel de riesgo es moderado; para el grado terciario se asigna 32% cuyo impacto es bajo y para el caso vacío no se

asigna ningún valor ya que no impacta a los criterios de información y no tiene nivel de riesgo.

Tabla 7

Resumen de proceso y criterios de información por impacto

Objetivos de control COBIT		Criterios de información del COBIT						
		Efectividad	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**
	Planear y organizar (PO)							
PO1	Definir un plan estratégico	**0.86**	**0.63**					
PO2	Definir la arquitectura de la información	**0.63**	**0.86**	**0.63**	**0.86**			
PO3	Determinar la dirección tecnológica	**0.86**	**0.86**					
PO6	Comunicar las aspiraciones y la dirección de la gerencia	**0.86**					**0.63**	
	Adquirir e implementar (AI)							
AI1	Identificar soluciones automatizadas	**0.86**	**0.63**					
AI2	Adquirir y mantener software aplicativo	**0.86**	**0.86**		**0.63**			**0.63**
AI3	Adquirir y mantener infraestructura tecnológica	**0.63**	**0.86**		**0.63**	**0.63**		
AI4	Facilitar la operación y el uso	**0.86**	**0.86**		**0.63**	**0.63**	**0.63**	**0.63**
	Dominio entregar y dar soporte (DS)							
DS4	Garantizar la continuidad del servicio	**0.86**	**0.63**			**0.86**		
DS5	Garantizar la seguridad de los sistemas			**0.86**	**0.86**	**0.63**	**0.63**	**0.63**
DS9	Administrar la configuración	**0.86**	**0.63**			**0.63**		**0.63**
DS10	Administración de programas	**0.86**	**0.86**			**0.63**		
DS11	Administración de datos				**0.86**			**0.86**
DS12	Administración de ambiente físico				**0.86**	**0.86**		
DS13	Administración de operaciones	**0.86**	**0.86**		**0.63**	**0.63**		
	Monitorear y evaluar (ME)							
ME1	Monitorear y evaluar el desempeño de TI	**0.86**	**0.86**	**0.63**	**0.63**	**0.63**	**0.63**	**0.63**

Elaborado por: Carmen Bastidas

El cálculo del impacto de los objetivos de control COBIT sobre los recursos y criterios TI, se determina multiplicando el grado de impacto por el nivel de madurez real que se encuentra el proceso y para el impacto por el nivel ideal se determina al multiplicar el grado de impacto por el nivel de madurez ideal el cual es 5.

Tabla 8

Tabla de impacto de los objetivos de control COBIT sobre los recursos y criterios TI (PO)

Objetivos de control COBIT		Criterios de información del COBIT							
Planear y organizar (PO)		**Efectividad**	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**	**Nivel de madurez**
PO1	Definir un plan estratégico	0,86	0,63						2
Impacto x nivel real		1,72	1,26						5
Impacto x nivel ideal		4,3	3,15						
PO2	Definir la arquitectura de la información	0,63	0,86	0,63	0,86				5
Impacto x nivel real		3,15	4,3	3,15	4,3				5
Impacto x nivel ideal		3,15	4,3	3,15	4,3				
PO3	Determinar la dirección tecnológica	0,86	0,86						2
Impacto x nivel real		1,72	1,72						5
Impacto x nivel ideal		4,3	4,3						
PO6	Comunicar las aspiraciones y la dirección de la gerencia	0,86					0,63		3
Impacto x nivel real		2,58					1,89		5
Impacto x nivel ideal		4,3					3,15		

Elaborado por: Carmen Bastidas

Tabla 9

Tabla de impacto de los objetivos de control COBIT sobre los recursos y criterios TI (AI)

Objetivos de control COBIT		Criterios de información del COBIT							
Adquirir e implementar (AI)		**Efectividad**	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**	**Nivel de madurez**
AI1	Identificar soluciones automatizadas	0,86	0,63						2
Impacto x nivel real		1,72	1,26						5
Impacto x nivel ideal		4,3	3,15						
AI2	Adquirir y mantener software aplicativo	0,86	0,86		0,63			0,63	3
Impacto x nivel real		2,58	2,58		1,89			1,89	5
Impacto x nivel ideal		4,3	4,3		3,15			3,15	
AI3	Adquirir y mantener infraestructura tecnológica	0,63	0,86		0,63	0,63			2
Impacto x nivel real		1,26	1,72		1,26	1,26			5
Impacto x nivel ideal		3,15	4,3		3,15	3,15			
AI4	Facilitar la operación y el uso	0,86	0,86		0,63	0,63	0,63	0,63	2
Impacto x nivel real		1,72	1,72		1,26	1,26	1,26	1,26	5
Impacto x nivel ideal		4,3	4,3		3,15	3,15	3,15	3,15	

Elaborado por: Carmen Bastidas

Tabla 10

Tabla de impacto de los objetivos de control COBIT sobre los recursos y criterios TI (DS)

Objetivos de control COBIT		Criterios de información del COBIT							
Dominio entregar y dar soporte (DS)		**Efectividad**	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**	**Nivel de madurez**
DS4	Garantizar la continuidad del servicio	0,86	0,63			0,86			1
Impacto x nivel real		0,86	0,63			0,86			5
Impacto x nivel ideal		4,3	3,15			4,3			
DS5	Garantizar la seguridad de los sistemas			0,86	0,86	0,63	0,63	0,63	4
Impacto x nivel real				3,44	3,44	2,52	2,52	2,52	5
Impacto x nivel ideal				4,3	4,3	3,15	3,15	3,15	
DS9	Administrar la configuración	0,86	0,63			0,63		0,63	2
Impacto x nivel real		1,72	1,26			1,26		0,63	5
Impacto x nivel ideal		4,3	3,15			3,15		3,15	
DS10	Administración de programas	0,86	0,86			0,63			3
Impacto x nivel real		2,58	2,58			1,89			5
Impacto x nivel ideal		12,9	12,9			9,45			
DS11	Administración de datos				0,86			0,86	2
Impacto x nivel real					1,72			1,72	5
Impacto x nivel ideal					4,3			4,3	
DS12	Administración de ambiente físico				0,86	0,86			4
Impacto x nivel real					3,44	3,44			5
Impacto x nivel ideal					4,3	4,3			
DS13	Administración de operaciones	0,86	0,86		0,63	0,63			2
Impacto x nivel real		1,72	1,72		1,26	1,26			5
Impacto x nivel ideal		4,3	4,3		3,15	3,15			

Elaborado por: Carmen Bastidas

Tabla 11

Tabla de impacto de los objetivos de control COBIT sobre los recursos y criterios TI (ME)

Objetivos de control COBIT		Criterios de información del COBIT							
Monitorear y evaluar (ME)		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Nivel de madurez
ME1	Monitorear y Evaluar el Desempeño de TI	0,86	0,86	0,63	0,63	0,63	0,63	0,63	3
Impacto x nivel real		2,58	2,58	1,89	1,89	1,89	1,89	1,89	5
Impacto x nivel ideal		4,3	4,3	3,15	3,15	3,15	3,15	3,15	

Elaborado por: Carmen Bastidas

Para sacar el total de los impactos reales e impactos ideales, se realiza la sumatoria de cada uno de los impactos correspondientes a cada proceso dando como resultado lo siguiente (mirar la tabla 10):

Tabla 12

Promedio de criterio de información

Total impacto x nivel real	**25,1**	**23,3**	**8,48**	**20,5**	**15,6**	**7,56**	**9,91**
Total impacto x nivel ideal	62,2	55,6	10,6	33	37	12,6	20,1
Porcentaje	41,3	42	80	62,1	42,3	60	49,4
Promedio de criterio de información			53,9 %				

Elaborado por: Carmen Bastidas

En la figura 12 se observan los resultados de los porcentajes obtenidos en la tabla 10, que da una idea de cómo los procesos impactan a cada uno de los criterios de información en los departamento analizados en Grupo El Comercio C.A.

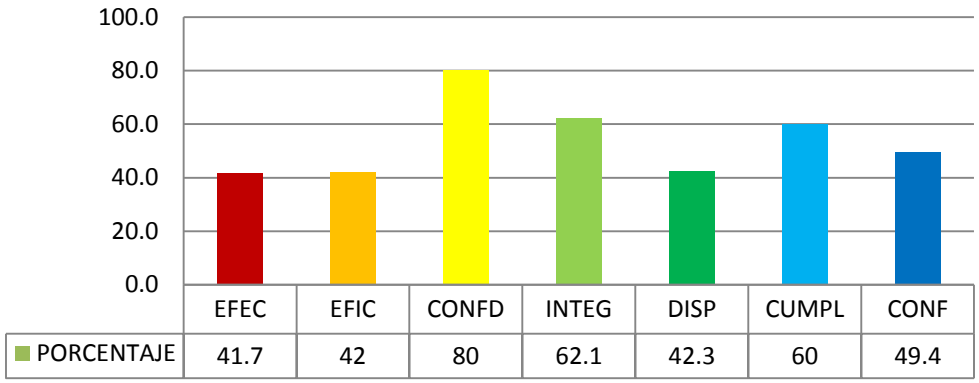


Figura 13. Representación gráfica de los resultados de porcentajes

Elaborado por: Carmen Bastidas

2.6 Selección de la muestra

Para encontrar información adecuada para la auditoría de los departamentos de Redacción y de Tecnología de Grupo El Comercio C.A., se realizará la selección de un grupo de personas que proporcione datos que reflejen el estado actual de sus áreas de trabajo.

De acuerdo al número de funcionarios que son 280 entre las dos áreas a auditar, es necesario aplicar una teoría de muestreo con enfoque matemático para la tabulación.

Ecuación 1

$$\boldsymbol{n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}}$$

Dónde:

N = tamaño de la población.

σ= Desviación estándar de la población, que generalmente cuando no se tiene su valor suele utilizarse un valor constante de 0,5.

Z = Valor obtenido mediante niveles de confianza. Es un valor constante que si no se tiene su valor, se lo toma en relación al 95% de confianza equivale a 1,96 (como más usual) o en relación al 99% de confianza equivale a 2,58, valor que queda a criterio del investigador.

e = Límite aceptable de error maestral, que generalmente cuando no se tiene su valor suele utilizarse un valor que varía entre el 1% (0,01) y 9% (0,09), valor que queda a criterio del encuestador.

$$n = \frac{280x(0{,}5)^2(2{,}27)^2}{(280-1)x\ (0{,}05)^2 + (0{,}5)^2 x\ 2{,}27^2}$$

$$n = \frac{360{,}703}{1{,}985725}$$

$$n = 181{,}648013$$

$$n = 182\ personas$$

Tabla 13

Porcentaje equivalente a cada uno de los encuestados

Personas	Porcentaje
182 personas	100%
18 personas rango alto	10%
164 usuarios	90%

Elaborado por: Carmen Bastidas

El tamaño de la muestra calculado corresponde a 182 personas que corresponde al 65% de la población total, los cuales serán encuestados bajo diferentes cuestionarios, lo que permitirá conocer el estado actual de la empresa; estado que se verá reflejado en los procesos del marco de referencia COBIT sujetos a la auditoría. (Ver anexos 1 y 2).

2.6.1 Análisis de resultados y modelos de madurez de los procesos

Para el análisis de resultados y la determinación del grado de madurez que se encuentra cada uno de los procesos COBIT de la empresa, se realizó tomando en cuenta los datos de la encuesta, determinando que el 10% corresponde a los jefes o altos mandos y el 90% a los usuarios, dando la suma de estos al 100% de los encuestados. Ver Anexo 3.

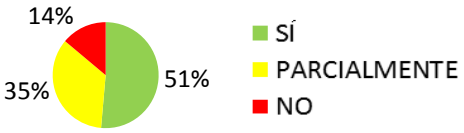
En las siguientes tablas se determinó el porcentaje que corresponde a cada pregunta; además se indica el grado de madurez y objetivos no cumplidos en cado uno de los procesos que establece COBIT; de igual manera las recomendaciones que se da para la mejora continua.

Tabla 14

Porcentaje equivalente al proceso PO1 y su nivel de madurez

Proceso PO1: Definir el plan estratégico de TI|

|JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
5	3	2	46	31	12	**TOTAL**	
						SÍ	51
						PARCIALMENTE	35
						|NO	14



Grado de madurez 2: Gestionado

La planeación estratégica de TI se comparte con la gerencia del negocio según se necesite. La actualización de los planes de TI ocurre como respuesta a las solicitudes de la dirección. Las decisiones estratégicas se toman proyecto por proyecto, sin ser consistentes con una estrategia global de la organización. Los riesgos y beneficios al usuario, resultado de decisiones estratégicas importantes, se reconocen de forma intuitiva.

Hallazgos:

Grupo El Comercio C.A. cuenta un Plan estratégico de TI parcialmente definido, ya que la razón de ser de las tecnologías de la información es el negocio y en este caso dichas perspectivas no se encuentran alineadas, es decir, no se administran de forma continua los planes tácticos; los sistemas implementados no están en su totalidad de acuerdo con los avances tecnológicos y no siguen un enfoque estructurado en el que dé a conocer a todo el equipo los planes estratégicos.

Recomendaciones:

- La planeación estratégica de TI debe tener integrado las estrategias del negocio y de TI definiendo planes de proyectos y evaluar las inversiones del portafolio, incluyendo el riesgo de no materializar los beneficios esperados.
- Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de contribución con los objetivos del negocio.
- Monitorear el proceso estratégico de TI para tomar decisiones de reingeniería de procesos del negocio.
- Actualizar de modo constante el proceso de planeación estratégica de TI desarrollando planes realistas a largo plazo de TI, impulsando la creación de nuevas capacidades de negocio a través de los avances tecnológicos, para así mejorar la ventaja competitiva de la organización.

Elaborado por: Carmen Bastidas

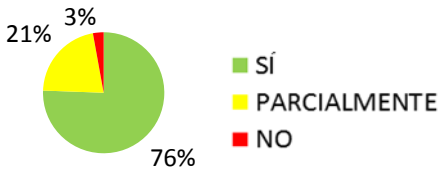
Tabla 15

Porcentaje equivalente al proceso PO2 y su nivel de madurez

Proceso PO2: Definir la arquitectura de la información

JEFES			USUARIOS			TOTAL
18			164			**182**
10%			90%			**100** **%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO	
4	3	3	0	19	71	

TOTAL	
SÍ	76
PARCIALMENTE	22
NO	3



Grado de madurez 3: Establecido

La importancia de la arquitectura de la información se entiende y se acepta, y la responsabilidad de su aplicación se asigna y se comunica de forma clara. Los procedimientos, herramientas y técnicas relacionados, aunque no son sofisticados, se han estandarizado y documentado. Se han desarrollado políticas básicas de arquitectura de información, incluyendo algunos requerimientos estratégicos, aunque el cumplimiento de políticas, estándares y herramientas no se refuerza de manera consistente. Existe una función de administración de datos definida formalmente, que establece estándares para toda la organización, y empieza a reportar sobre la aplicación y uso de la arquitectura de la información.

Hallazgos:

Grupo El Comercio C.A. no dispone de un diccionario corporativo de datos y tiene parcialmente definidos procesos y herramientas para garantizar la integridad de datos.

Recomendaciones:

- Desarrollar un diccionario corporativo de datos que optimice el uso de la información.
- Definir y dar mantenimiento a una arquitectura de información para que refleje todos los requerimientos del negocio garantizando la integridad y consistencia de los datos.

Elaborado por: Carmen Bastidas

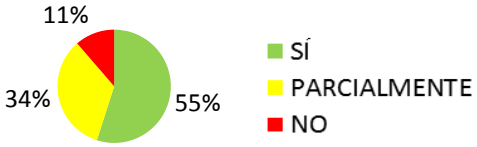
Tabla 16

Porcentaje equivalente al proceso PO3 y su nivel de madurez

Proceso PO3: Determinar la dirección tecnológica

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
6	4	0	49	30	11		

TOTAL	
SÍ	55
PARCIALMENTE	34
NO	11



Grado de madurez 3: Establecido

Existe un plan de infraestructura tecnológica definido, documentado y bien difundido, aunque se aplica de forma inconsistente. La orientación de la infraestructura tecnológica incluye el entendimiento de dónde la empresa desea ser líder y dónde desea rezagarse respecto al uso de tecnología, con base en los riesgos y en la alineación con la estrategia organizacional.

Hallazgos:

Para la implementación del plan de infraestructura que posee Grupo El Comercio C.A. se han planteado parcialmente estándares y directrices para la arquitectura de la información. El plan no se actualiza de forma regular y no están integrados en su totalidad los servicios de TI de acuerdo con los requerimientos y prioridades del negocio, actuales y futuros.

Recomendaciones:

- Se debe tomar en cuenta el impacto potencial de las tecnologías cambiantes y emergentes en el desarrollo del plan de infraestructura, para garantizar que el equipo de TI pueda administrar dichos cambios.
- Definir un proceso continuo y reforzado para mejorar el plan de infraestructura tecnológica tomando en cuenta planes estratégicos y tácticos de TI, estándares y avances industriales e internacionales, en lugar de estar orientado por los proveedores de la tecnología, para crear potenciales oportunidades en el negocio.

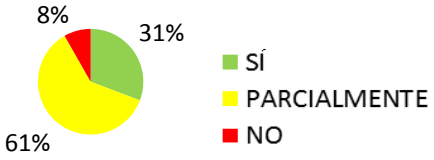
Elaborado por: Carmen Bastidas

Tabla 17

Porcentaje equivalente al proceso PO6 y su nivel de madurez

Proceso PO6: Comunicar las aspiraciones y la dirección de la gerencia

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
4	6	0	27	55	8	**TOTAL**	
						SÍ	31
						PARCIALMENTE	61
						NO	8



Grado de madurez 3: Establecido

La gerencia ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información, que incluye un marco para las políticas, procedimientos y estándares, cuyo proceso de elaboración es estructurado, mantenido y conocido por el personal aunque no se aplique de forma rigurosa, ya que el monitoreo del cumplimiento de estas políticas y estándares es inconsistente.

Hallazgos:

El ambiente de control de la información está alineado parcialmente con el marco administrativo, estratégico de la empresa y las políticas de control interno; no son conocidas ampliamente por todos los usuarios de la organización.

La organización como tal no entrega periódicamente un reporte de responsabilidad social corporativa.

Recomendaciones:

- Asegurarse que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunique a los usuarios de la organización, para que tengan en cuenta lo que deben hacer para apoyar el logro de los mismos.
- Alinear el ambiente de control de la información con el marco administrativo estratégico y con la visión, para que con frecuencia se revise, actualice y se mejore.
- Adoptar las mejores prácticas con respecto a las técnicas de comunicación monitoreando así la autoevaluación y las verificaciones del marco de control empresarial de TI.

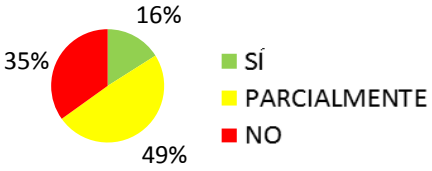
Elaborado por: Carmen Bastidas

Tabla 18

Porcentaje equivalente al proceso AI1 y su nivel de madurez

Proceso AI1: Identificar soluciones automatizadas

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
5	3	2	11	46	33	**TOTAL**	
						SÍ	16
						PARCIALMENTE	49
						NO	35



Grado de madurez 2: Gestionado

Las soluciones se identifican de manera informal con base en la experiencia interna y en el conocimiento de la función de TI. El éxito de cada proyecto depende de la experiencia de unos cuantos individuos claves. La calidad de la documentación y la toma de decisiones varían de forma considerable. Se usan enfoques no estructurados para definir los requerimientos e identificar las soluciones tecnológicas.

Hallazgos:

Para implementar las soluciones automatizadas que tiene Grupo El Comercio C.A. no se había realizado adecuadamente un estudio de viabilidad, ya que no cumplen del todo con los requerimientos del negocio.

No se evalúa periódicamente si las soluciones adquiridas cumplen con los objetivos del negocio, ya que en ocasiones ha ameritado un cambio significativo de algún requerimiento tecnológico.

Se tiene parcialmente información documentada de riegos relacionados a requerimientos técnicos, funcionales y de estudios de factibilidad.

Recomendaciones:

- Identificar soluciones que sean técnicamente factibles y rentables, para tomar la decisión de elección de la solución automatizada y al enfoque de adquisición tomando la decisión de "compra vs. desarrollo", que optimice el valor y minimice los riesgos.
- Realizar un estudio de viabilidad de soluciones automatizadas antes de implementarlas, para que así estas se conviertan en soluciones efectivas y eficientes, que satisfagan las estrategias de la organización y de TI para tener usuarios satisfechos con la funcionalidad recibida.
- Evaluar las soluciones de TI a través de reportes de análisis de riesgos para que así dicho procedimiento esté sujeto a una mejora continua.

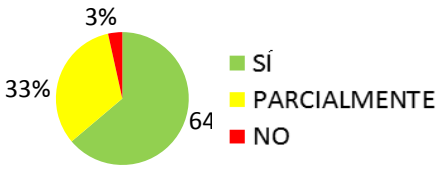
Elaborado por: Carmen Bastidas

Tabla 19

Porcentaje equivalente al proceso AI2 y su nivel de madurez

Proceso AI2: Adquirir y mantener software aplicativo

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
3	3	3	60	30	0	**TOTAL**	
						SÍ	64
						PARCIALMENTE	33
						NO	3



Grado de madurez 3: Establecido

Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Este proceso va de acuerdo con la estrategia de TI y del negocio.

Hallazgos:

Las aplicaciones con las que cuenta Grupo El Comercio C.A. se encuentran parcialmente licenciadas, ya que la misma no cuenta con un sistema de control que le permita auditar las aplicaciones; por ende no se ha verificado que el software cumpla con las debidas regulaciones, ya que la empresa no posee un plan de revisión postimplementación para cada sistema de información.

Recomendaciones:

- Elaborar un plan de adquisición y mantenimiento de software integrado y estandarizado, que garantice la mejor toma de decisiones para conseguir los objetivos de negocio.
- Separar actividades de desarrollo, pruebas y operación para la documentación.
- Definir un plan de aseguramiento de calidad del software aplicativo adquirido, desarrollado y ejecutado.
- Contar con un inventario de software donde se registren todos los datos del software adquirido.

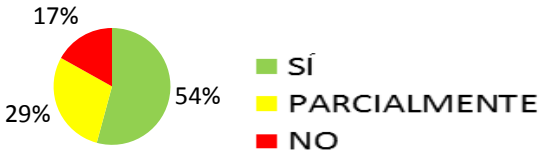
Elaborado por: Carmen Bastidas

Tabla 20

Porcentaje equivalente al proceso AI3 y su nivel de madurez

Proceso AI3: Adquirir y mantener infraestructura tecnológica

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
6	2	1	48	27	16	**TOTAL**	
						SÍ	54
						PARCIALMENTE	29
						NO	17



Grado de madurez 2: Gestionado

La adquisición y mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que se deben respaldar. Algunos mantenimientos se programan, pero no se programa ni se coordina en su totalidad.

Hallazgos:

La infraestructura tecnológica actual de la empresa responde parcialmente a las necesidades de la misma, ya que no se realizan controles regulares para confirmar si se está o no alineado con los requerimientos de la empresa, medición de debilidades y exigencias de seguridad.
No están establecidas pruebas de integración y desempeño, es decir, migración entre ambientes.

Recomendaciones:

- Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y software de la infraestructura, para proteger los recursos y garantizar su disponibilidad e integridad.
- Establecer un plan de mantenimiento de infraestructura confiable y segura, para garantizar que se controlan los cambios de acuerdo con el procedimiento de administración de cambios de la organización.
- Optimizar el proceso de adquisición y mantenimiento de la infraestructura de tecnología, para que esté alineado con las aplicaciones críticas del negocio y con la arquitectura de la tecnología.

Elaborado por: Carmen Bastidas

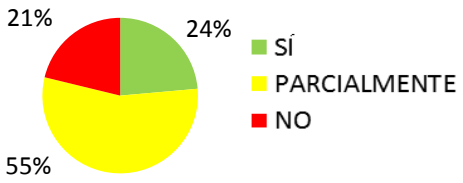
Tabla 21

Porcentaje equivalente al proceso AI4 y su nivel de madurez

Proceso AI4: Facilitar la operación y el uso

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
0	4	6	24	51	15	**TOTAL**	

SÍ	24
PARCIALMENTE	55
NO	21



Grado de madurez 2: Gestionado

No hay un enfoque uniforme o estructurado para generar procedimientos y documentación. Los procesos relacionados con la calidad de apoyo al usuario está en el rango de muy pobre a muy buena, pero su estabilidad e integración es bastante baja en toda la compañía.

Se proporcionan o facilitan programas de entrenamiento para el negocio y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento.

Hallazgos:

La organización no cuenta con un procedimiento formal para realizar la transferencia del conocimiento tanto a la gerencia como a usuarios finales y personal de operación y soporte.

Se informa parcialmente de los cambios y actualizaciones a realizarse en los sistemas.

Recomendaciones:

- Proporcionar manuales de operación de los sistemas a los usuarios para transferir el conocimiento necesario para el uso exitoso del sistema.
- Poner en conocimiento las actualizaciones que se vayan hacer en los sistemas de forma clara y oportuna, para garantizar así el correcto uso y operación de los mismos.

Elaborado por: Carmen Bastidas

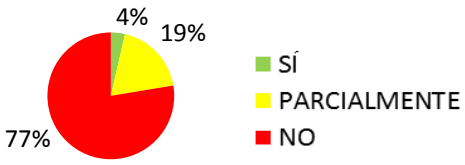
Tabla 22

Porcentaje equivalente al proceso DS4 y su nivel de madurez

Proceso DS4: Garantizar la continuidad del servicio

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
4	2	4	0	16	74	**TOTAL**	

SÍ	4
PARCIALMENTE	19
NO	78



Grado de madurez 1: Ejecutado

Las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada.

Hallazgos:

Dentro de la organización existe parcialmente un marco de continuidad de TI debido a que no existe una asignación de responsabilidades para actividades en caso de algún altercado que interrumpa la continuidad del negocio; a más de ello, no hay una debida comunicación a los usuarios de los planes que implica dicho marco de continuidad.

En cuando al medio ambiental, que es un factor importante, no existe ninguna medida preventiva de posibles errores en el futuro.

Recomendaciones:

- Desarrollar planes de contingencia de TI tomando en cuenta referencias de la industria y las mejores prácticas externas para que puedan ejecutarse, probarse y mantenerse, para así asegurar un mínimo impacto al negocio en caso de una interrupción o cambio en los servicios de TI.
- Documentar estructuradamente el plan de continuidad para que sea difundido de manera apropiada y segura a todos los involucrados, los cuales deben tener claro la ruta de escalamiento.
- Realizar un control continuo del estado de los equipos de infraestructura, para asegurar que puedan resistir y recuperarse de fallas originadas, ya sea por un ataque deliberado o un desastre natural.
- Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio.

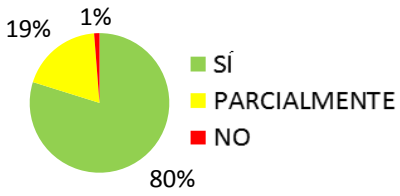
Elaborado por: Carmen Bastidas

Tabla 23

Porcentaje equivalente al proceso DS5 y su nivel de madurez

Proceso DS5: Garantizar la seguridad de los sistemas

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
5	4	1	0	15	75	**TOTAL**	
						SÍ	80
						PARCIALMENTE	19
						NO	1



Grado de madurez 4: Predecible

Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. La familiaridad con normas que conciencien sobre la importancia de la seguridad es obligatoria.La identificación, autenticación y autorización de los usuarios está estandarizada.

Hallazgos:

El plan de seguridad está parcialmente alineado con las políticas de la empresa.

No existen medidas preventivas, detectivas ni correctivas en la organización, así como tampoco se genera reportes de incidentes de los sistemas de información.

Recomendaciones:

- Identificar, monitorear y reportar vulnerabilidades e incidentes de seguridad generando informes para minimizar el impacto que estos produzcan en la seguridad de los sistemas.
- Mantener la integridad de la información y de la infraestructura de procesamiento, recolectando e implementando de forma oportuna controles adecuados para mitigar riesgos para la mejora continua de procesos.
- La seguridad en TI debe ser alineada con las políticas del negocio.

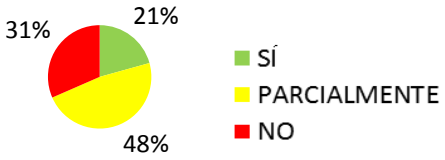
Elaborado por: Carmen Bastidas

Tabla 24

Porcentaje equivalente al proceso DS9 y su nivel de madurez

Proceso DS9: Administrar la configuración

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
6	1	3	15	47	29	**TOTAL**	
						SÍ	21
						PARCIALMENTE	48
						NO	32



Grado de madurez 2: Gestionado

La gerencia es consciente de la importancia de la configuración de TI. Además, comprende las ventajas de conservar toda la información sobre las configuraciones; sin embargo, existe una dependencia latente del conocimiento y de la experiencia del personal técnico.

Además no se han definido prácticas estandarizadas de trabajo. Debido a que los datos que se tiene de la configuración son limitados, no lo usan los métodos interrelacionados, como la administración de cambios y la de problemas.

Hallazgos:

El control de inventario que maneja Grupo El Comercio C.A. está parcialmente actualizado, ya que no se han comparado las configuraciones de los activos con el registro de configuraciones de software y hardware existentes en el inventario.

Recomendaciones:

- Establecer y mantener un repositorio completo de la configuración de los activos, revisarlo periódicamente para verificar y confirmar la integridad de los datos.
- La exploración de activos, así como la inspección de activos individuales de IT, están resguardadas de hurto, uso indebido y abuso.

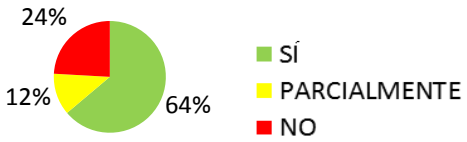
Elaborado por: Carmen Bastidas

Tabla 25

Porcentaje equivalente al proceso DS10 y su nivel de madurez

Proceso DS10: Administración de problemas

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
1	5	4	63	7	20	**TOTAL**	
						SÍ	64
						PARCIALMENTE	12
						NO	24



Grado de madurez 3: Establecido

Se acepta la necesidad de un sistema integrado de administración de problemas y se evidencia con el apoyo de la Gerencia. Se estandarizan los procesos de escalamiento y resolución de problemas. De la búsqueda de conflictos y sus respectivas soluciones, se encarga el equipo de respuesta, empleando los recursos disponibles, sin monopolizar. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitadas e informales.

Hallazgos:

Grupo El Comercio C.A. maneja una administración cuyos problemas son categorizados parcialmente por procesos reportados, en donde no se tiene un tiempo determinado para solucionarlos.

No se han establecido procedimientos para el monitoreo de los problemas encontrados, ya que la acción que se ha tomado en relación a los servicios afectados es que en cuanto recuperan su estatus normal se procede parcialmente al cierre del mismo.

Recomendaciones:

- Clasificar adecuadamente los problemas reportados de acuerdo a: categoría, impacto, urgencia y prioridad, para que de tal manera se pueda determinar la causa raíz de los mismos, obteniendo reportes del progreso en la resolución de problemas o errores.
- Ajustar el proceso de administración de problemas a un proceso proactivo y preventivo, que contribuye con los objetos de TI, en donde se debe documentar, comunicar y medir problemas pasados y futuros, a través de contactos regulares con proveedores.

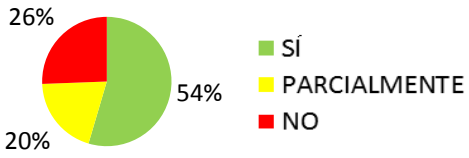
Elaborado por: Carmen Bastidas

Tabla 26

Porcentaje equivalente al proceso DS11 y su nivel de madurez

Proceso DS11: Administración de datos

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
1	2	7	54	18	19	**TOTAL**	
						SÍ	55
						PARCIALMENTE	20
						NO	26



Grado de madurez 2: Gestionado

A lo largo de toda la organización existe conciencia sobre la necesidad de una adecuada administración de los datos. Las demandas de seguridad para el correcto manejo de datos son almacenados por personal clave. Se efectúa por medio de un monitoreo de TI sobre las labores de la administración de datos, tales como: eliminación, respaldo, recuperación…

Hallazgos:

Grupo El Comercio C.A. cuenta parcialmente con políticas para el respaldo de datos alineados con los requerimientos del negocio, es decir, que no cuenta del todo con un plan de seguridad para la administración de los datos de los diferentes sistemas y aplicaciones.

El respaldo de datos no es una labor automatizada.

No se cuenta con alguna metodología para deshacerse de datos que ya no se necesitan.

Recomendaciones:

- Realizar un plan de respaldos para optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera, es decir, respaldando los datos y probando la restauración de la información de forma efectiva y eficiente para conseguir los objetivos de negocio, la política de seguridad de la organización y los requerimientos regulatorios. Todo esto debe ser asignado a la parte responsable que controla la integridad y la seguridad de la administración de datos.
- Establecer una metodología para desechar de manera segura los datos y el equipo para que no puedan ter acceso personas que pueden hacer mal uso de la información.
- Una vez establecida la responsabilidad sobre la administración de los datos, dichos procedimientos se formalizan dentro de TI, y se debería utilizar herramientas con un máximo de automatización de la administración de los datos

Elaborado por: Carmen Bastidas

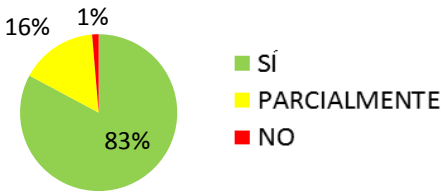
Tabla 27

Porcentaje equivalente al proceso DS12 y su nivel de madurez

Proceso DS12: Administración del ambiente físico

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
6	2	1	76	14	0		

TOTAL	
SÍ	83
PARCIALMENTE	16
NO	1



Grado de madurez 4: Predecible

A través de diferentes normas se determinan los términos de un convenio, que abarca el alcance de trabajo, gastos, facilidades de facturación, cronograma, responsabilidades, etc.Se asignan las responsabilidades para la administración del contrato y del proveedor. Las aptitudes, capacidades y riesgos del proveedor son verificadas de forma continua. Las características del servicio están acordes con las metas de la organización. Así mismo, la empresa posee un proceso de medición que le ayuda a obtener información del desempeño y los términos contractuales; esto le abastece de un conocimiento más exacto de los servicios actuales. Se utilizan modelos de fijación de precios de transferencia en el proceso de adquisición. Todas las partes involucradas tienen conocimiento de las expectativas del servicio, de los costos y de las etapas.

Hallazgos:

No se diseñaron e implementaron medidas de protección contra factores ambientales.

Se definieron parcialmente procedimientos para controlar el acceso al ambiente físico, donde existe información crítica.

Recomendaciones:

- Diseñar e implementar medidas de protección contra factores ambientales instalando dispositivos y equipo especializado para monitorear y controlar el ambiente, para garantizar que los servicios y la infraestructura de TI puedan resistir y recuperarse de forma apropiada.
- Definir procedimientos para el acceso al ambiente físico, cuyo acceso debería justificarse, autorizarse, registrarse y monitorearse de acuerdo con los requerimientos del negocio, minimizando así el riesgo de interrupción del servicio.

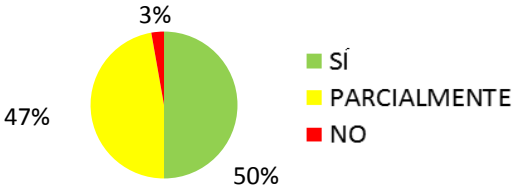
Elaborado por: Carmen Bastidas

Tabla 28

Porcentaje equivalente al proceso DS13 y su nivel de madurez

Proceso DS13: Administración del operaciones

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
50	47	3	0	0	0	**TOTAL**	
						SÍ	50
						PARCIALMENTE	47
						NO	3



Grado de madurez 2: Gestionado

La organización está consciente del rol clave que las actividades de operaciones de TI juegan en brindar funciones de soporte de TI, las mismas que son informales e intuitivas. Se asignan presupuestos para herramientas con un criterio de caso por caso. Hay una alta dependencia sobre las habilidades de los individuos. Las instrucciones de qué hacer, cuándo y en qué orden no están documentadas. Existe algo de habilitación para el operador y hay algunos estándares de operación formales.

Hallazgos:

Se entregan parcialmente los servicios de TI de acuerdo con las prioridades del negocio y esto implica que las operaciones de TI no son del todo eficientes, efectivas y flexibles para cumplir con las necesidades de niveles de servicio con una pérdida de productividad mínima.

Recomendaciones:

- Soportar las operaciones a través de presupuestos de recursos para prioridades del negocio, asegurándose que los servicios de TI están disponibles conforme se requieren.
- Las programaciones y las tareas deben ser documentadas y comunicadas de manera formal, tanto a la función interna de TI como a los usuarios finales, garantizando la satisfacción de ellos.
- Definir procedimientos de operación de mejora continua y alinearlos con los niveles operativos de servicio para procesamiento de datos programados (herramientas de automatización para limitar la intervención del operador), protección de datos, monitoreo y mantenimiento de la infraestructura de TI, garantizando así que pueda recuperarse de fallas ocasionadas por errores, ataques deliberados o desastres.
- Establecer reuniones periódicas con los responsables de administración de operaciones, para garantizar la inclusión oportuna de cambios en las programaciones de producción, en colaboración con los proveedores.

Elaborado por: Carmen Bastidas

Tabla 29

Porcentaje equivalente al proceso ME1 y su nivel de madurez

Proceso ME1: Monitorear y evaluar el desempeño de TI

JEFES			USUARIOS			TOTAL	
18			164			**182**	
10%			90%			**100**	**%**
SÍ	PARCIALMENTE	NO	SÍ	PARCIALMENTE	NO		
72	28	0	0	0	0	**TOTAL**	
						SÍ	72
						PARCIALMENTE	28
						NO	0

Grado de madurez 3: Establecido

La gerencia se ha preocupado por comunicar y oficializar acerca de un proceso de monitoreo. También se han elaborado programas de capacitación y entrenamiento para este proceso. Las evaluaciones todavía se realizan al nivel de procesos y proyectos individuales de TI y no están integradas a través de todos los procesos. Se han definido herramientas para monitorear los procesos y los niveles de servicio de TI.

Hallazgos:

El método de monitoreo que tiene establecido actualmente Grupo El Comercio C.A. hace un análisis parcial de todos los ángulos de los procesos de TI.

Parcialmente se realizan reportes para que los altos mandos de la organización se enteren del estado de cumplimiento de las metas.

Recomendaciones:

- Establecer un monitoreo que brinde una visión precisa desde todos los ángulos de desempeño, con un proceso de mejora continua, actualizando los estándares y las políticas a nivel organizacional incorporando mejores prácticas de la industria.
- Traducir los reportes de desempeño de procesos a reportes administrativos, para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño.

Elaborado por: Carmen Bastidas

A continuación se presenta un reporte general de cada uno de los procesos y en qué grado de madurez se encuentran.

Tabla 30

Reporte general de los grados de madurez

Dominio	Proceso	Grado de madurez
	Planear y organizar (PO)	
PO1	Definir un plan estratégico	**2**
PO2	Definir la arquitectura de la información	**5**
PO3	Determinar la dirección tecnológica	**2**
PO6	Comunicar las aspiraciones y la dirección de la Gerencia	**3**
	Adquirir e implementar (AI)	
AI1	Identificar soluciones automatizadas	**2**
AI2	Adquirir y mantener software aplicativo	**3**
AI3	Adquirir y mantener infraestructura tecnológica	**2**
AI4	Facilitar la operación y el uso	**2**
	Entregar y dar soporte (DS)	
DS4	Garantizar la continuidad del servicio	**1**
DS5	Garantizar la seguridad de los sistemas	**4**
DS9	Administrar la configuración	**2**
DS10	Administración de programas	**3**
DS11	Administración de datos	**2**
DS12	Administración de ambiente físico	**4**
DS13	Administración de operaciones	**2**
	Monitorear y evaluar (ME)	
ME1	Monitorear y evaluar el desempeño de TI	**3**

Elaborado por: Carmen Bastidas

CAPÍTULO 3

INFORME TÉCNICO Y EJECUTIVO

3.1 Informe técnico

INFORME TÉCNICO	
"PLAN DE AUDITORÍA INFORMÁTICA PARA GRUPO EL COMERCIO C.A., CON APLICACIÓN DE LA METODOLOGÍA COBIT 4.1"	UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

En el presente informe se describirá el resultado del proceso de evaluación como parte de la auditoría realizado a los departamentos de Redacción y de Tecnología, en base a los grados de madurez, los cuales van desde el grado 0 (no existente) al grado máximo 5 (administrado) de la gestión de las TICs, para emitir las respectivas recomendaciones para cada uno de los procesos seleccionados divididos en sus respectivos dominios (Planear y organizar, Adquirir e implementar, Entregar y dar soporte, Monitorear y evaluar) de COBIT.

Alcance:

Mediante la Auditoría a los departamentos de Redacción y de Tecnología se pretende evaluar el estado actual determinando el nivel de cumplimiento de cada proceso, y de esta manera brindar a Grupo El Comercio C.A. sus respectivas conclusiones y recomendaciones para cada uno de los procesos evaluados en cada dominio, según la metodología COBIT 4.1, para contribuir al alcance de los objetivos del negocio.

Objetivos:

Objetivo general:

- Realizar un Plan de Auditoría para el Grupo El Comercio C.A., con aplicación de la Metodología COBIT 4.1.

Objetivos específicos:

- Recopilar información de la seguridad física y lógica de los diversos ambientes de procesamiento de la misma.
- Estudiar y seleccionar los procesos del marco de trabajo COBIT apropiados para Grupo El Comercio C.A.
- Realizar la auditoría estableciendo el grado de madurez actual de acuerdo con los modelos de COBIT.

<table>
<tr><td colspan="2">A continuación se detallan las observaciones y recomendaciones resultantes de la revisión en base al estándar COBIT</td></tr>
<tr><td colspan="2">Dominio: Planear y organizar</td></tr>
<tr><td>Procesos</td><td>Niveles de madurez</td></tr>
<tr><td rowspan="4">PO1: Definir un plan estratégico de TI</td><td>Actual: Nivel 2</td></tr>
<tr><td>Grupo el Comercio C.A. cuenta un Plan estratégico de TI parcialmente definido, ya que no se administran de forma continua los planes tácticos. Los sistemas implementados no están en su totalidad de acuerdo con los avances tecnológicos y no sigue un enfoque estructurado en el que dé a conocer a todo el equipo los planes estratégicos.</td></tr>
<tr><td>Recomendado: Nivel 4</td></tr>
<tr><td>• Integrar y actualizar las estrategias del negocio y de TI en el Plan estratégico definiendo planes de proyectos e inversiones del portafolio que vayan acorde a los avances tecnológicos, para mejorar así la ventaja competitiva de la organización. Dicho plan deber ser documentado y comunicado a toda la empresa.
• Evaluar y monitorear el desempeño de los planes existentes y de los sistemas de información en términos de contribución con los objetivos del negocio.</td></tr>
<tr><td>Procesos</td><td>Niveles de madurez</td></tr>
<tr><td rowspan="4">PO2: Definir la arquitectura de la información</td><td>Actual: Nivel 3</td></tr>
<tr><td>Grupo El Comercio C.A. no dispone de un diccionario corporativo de datos y tiene parcialmente definidos procesos y herramientas para garantizar la integridad de datos.</td></tr>
<tr><td>Recomendado: Nivel 4</td></tr>
<tr><td>• Desarrollar un diccionario corporativo de datos que optimice el uso de la información.
• Definir y dar mantenimiento a una arquitectura de información para que refleje todos los requerimientos del negocio garantizando la integridad y consistencia de los datos.</td></tr>
</table>

Procesos	Niveles de madurez
PO3: Determinar la dirección tecnológica	**Actual: Nivel 3**
	Para la implementación del plan de infraestructura que posee Grupo El Comercio C.A. se han planteado parcialmente estándares y directrices para la arquitectura de la información. El plan no se actualiza de forma regular y no están integrados en su totalidad los servicios de TI de acuerdo con los requerimientos y prioridades del negocio, actuales y futuros.
	Recomendado: Nivel 4
	• Definir un proceso continuo y reforzado para mejorar y dar mantenimiento al plan de infraestructura tecnológica, tomando en cuenta planes estratégicos y tácticos de TI, estándares y avances industriales e internacionales, en lugar de estar orientado por los proveedores de la tecnología, para crear potenciales oportunidades en el negocio.
Procesos	**Niveles de madurez**
PO6: Comunicar las aspiraciones y la dirección de la gerencia	**Actual: Nivel 3**
	El ambiente de control de la información está alineado parcialmente con el marco administrativo, estratégico de la empresa y las políticas de control interno; no son conocidas ampliamente por todos los usuarios de la organización. La organización como tal no entrega periódicamente un reporte de responsabilidad social corporativa.
	Recomendado: Nivel 4
	• Alinear el ambiente de control de la información con el marco administrativo estratégico y con la visión, para que con frecuencia se revise, actualice y se mejore. • Asegurarse que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunique a los usuarios de la organización, para que tengan en cuenta qué deben hacer para apoyar el logro de los mismos.

Procesos	Niveles de madurez
AI1: Identificar soluciones automatizadas	**Actual: Nivel 2**
	Para implementar las soluciones automatizadas que tiene Grupo El Comercio C.A. no se había realizado adecuadamente un estudio de viabilidad, ya que no cumple del todo con los requerimientos del negocio. No se evalúa periódicamente si las soluciones adquiridas cumplen con los objetivos del negocio, ya que en ocasiones ha ameritado un cambio significativo de algún requerimiento tecnológico. Se tiene parcialmente información documentada de riegos relacionados a requerimientos técnicos, funcionales y de estudios de factibilidad.
	Recomendado: Nivel 4
	• Realizar un estudio de viabilidad debidamente documentado en el que consten soluciones automatizadas que sean técnicamente factibles y rentables antes de implementarlas, para que así estas se conviertan en soluciones efectivas y eficientes que satisfagan las estrategias de la organización y de TI para tener usuarios satisfechos con la funcionalidad recibida. • Evaluar las soluciones de TI a través de reportes de análisis de riesgos para que así dicho procedimiento esté sujeto a una mejora continua.
Procesos	**Niveles de madurez**
AI2: Adquirir y mantener software aplicativo	**Actual: Nivel 3**
	Las aplicaciones con las que cuenta Grupo El Comercio C.A. se encuentran parcialmente licenciadas, ya que la misma no cuenta con un sistema de control que le permita auditar las aplicaciones; por ende no se ha verificado que el software cumpla con las debidas regulaciones, ya que la empresa no posee un plan de revisión postimplementación para cada sistema de información.
	Recomendado: Nivel 4
	• Elaborar un plan de adquisición y mantenimiento de software integrado y estandarizado que incluya un proceso de diseño y especificación, un criterio de adquisición y un proceso de prueba que garantice la mejor toma de decisiones para conseguir los objetivos de negocio. • Contar con un inventario de software donde se registren todos los datos del software adquirido.

Procesos	Niveles de madurez
AI3: Adquirir y mantener infraestructura tecnológica	**Actual: Nivel 2**
	La infraestructura tecnológica actual de la empresa responde parcialmente a las necesidades de la misma, ya que no se hacen revisiones periódicas para evaluar si se está alineado con las necesidades del negocio, evaluación de vulnerabilidades y requerimientos de seguridad. No están establecidas pruebas de integración y desempeño, es decir, migración entre ambientes.
	Recomendado: Nivel 4
	• Establecer un proceso claro y definido para adquirir y dar mantenimiento a la infraestructura de TI a tal punto que funcione bien para la mayoría de las situaciones, dándole un seguimiento consistente para que concuerde con las estrategias del negocio.
Procesos	**Niveles de madurez**
AI4: Facilitar la operación y el uso	**Actual: Nivel 2**
	La organización no cuenta con un procedimiento formal para realizar la transferencia del conocimiento, tanto a la gerencia como a usuarios finales y personal de operación y soporte. Se informa parcialmente de los cambios y actualizaciones a realizarse en los sistemas.
	Recomendado: Nivel 4
	• Proporcionar manuales de operación de los sistemas a los usuarios para transferir el conocimiento necesario para el uso exitoso del sistema. • Poner en conocimiento las actualizaciones que se vayan hacer en los sistemas de forma clara y oportuna, para garantizar así el correcto uso y operación de los mismos.

Procesos	Niveles de madurez
DS4: Garantizar la continuidad del servicio	**Actual: Nivel 1**
	Dentro de la organización existe parcialmente un marco de continuidad de TI debido a que no existe una asignación de responsabilidades para actividades en caso de algún altercado que interrumpa la continuidad del negocio; a más de ello no hay una debida comunicación a los usuarios de los planes que implica dicho marco de continuidad. En cuando al medio ambiental, que es un factor importante, no existe ninguna medida preventiva de posibles errores en el futuro.
	Recomendado: Nivel 4
	• Desarrollar planes de contingencia que estén debidamente establecidos y documentados de manera apropiada, tomando en cuenta referencias de la industria y las mejores prácticas externas para que puedan ejecutarse, probarse y mantenerse, para así asegurar un mínimo impacto al negocio en caso de una interrupción o cambio en los servicios de TI. • Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio.
Procesos	**Niveles de madurez**
DS5: Garantizar la seguridad de los sistemas	**Actual: Nivel 4**
	El plan de seguridad está parcialmente alineado con las políticas de la empresa. No existen medidas detectivas, correctivas en la organización y tampoco se generan reportes de incidentes de los sistemas de información.
	Recomendado: Nivel 4
	• Identificar, monitorear y reportar vulnerabilidades e incidentes de seguridad generando reportes para minimizar el impacto que estos produzcan en la seguridad de los sistemas. • La seguridad en TI deben ser alineados con las políticas del negocio.

Procesos	Niveles de madurez
DS9: Administrar la configuración	**Actual: Nivel 2**
	El control de inventario que maneja Grupo El Comercio C.A. está parcialmente actualizado, ya que no se han comparado las configuraciones de los activos con el registro de configuraciones de software y hardware existentes en el inventario.
	Recomendado: Nivel 4
	• Establecer un proceso de automatización para ayudar a rastrear cambios en el software y hardware, para que de tal manera se mantenga un repositorio completo de la configuración de los activos, revisarlo periódicamente para verificar y confirmar la integridad de los datos.
Procesos	**Niveles de madurez**
DS10: Administración de programas	**Actual: Nivel 3**
	Grupo El Comercio C.A. maneja una administración cuyos problemas son categorizados parcialmente por procesos reportados, en donde no se tiene un tiempo determinado para solucionarlos. No se han establecido procedimientos para el monitoreo de los problemas encontrados, ya que la acción que se ha tomado en cuanto a los servicios afectados es que en cuanto recuperan su estatus normal se procede parcialmente al cierre del mismo.
	Recomendado: Nivel 4
	• Clasificar adecuadamente los problemas reportados de acuerdo a: categoría, impacto, urgencia y prioridad para que de tal manera se pueda determinar la causa raíz de los mismos, obteniendo reportes del progreso en la resolución de problemas o errores. • Ajustar el proceso de administración de problemas a un proceso proactivo y preventivo, que contribuye con los objetos de TI, en donde se debe documentar, comunicar y medir problemas pasados y futuros, a través de contactos regulares con proveedores.

Procesos	Niveles de madurez
DS11: Administración de datos	**Actual: Nivel 2**
	Grupo El Comercio C.A. cuenta parcialmente con políticas para el respaldo de datos alineados con los requerimientos del negocio, es decir, que no cuenta del todo con un plan de seguridad para la administración de los datos de los diferentes sistemas y aplicaciones. El respaldo de datos no es una labor automatizada. No se cuenta con alguna metodología para deshacerse de datos que ya no se necesitan.
	Recomendado: Nivel 4
	• Realizar un plan de respaldos para optimizar el uso de la información y garantizar la disponibilidad de la misma cuando se requiera, cumpliendo así con la política de seguridad de la organización y los requerimientos regulatorios. Todo esto debe ser asignado a la parte responsable que controla la integridad y la seguridad de la administración de datos; dicho procedimiento debe ser formalizado dentro de TI, considerando la utilización de herramientas para la automatización de la administración de los datos.
Procesos	**Niveles de madurez**
DS12: Administración del ambiente físico	**Actual: Nivel 4**
	No se diseñaron e implementaron medidas de protección contra factores ambientales. Se definieron parcialmente procedimientos para controlar el acceso al ambiente físico donde existe información crítica.
	Recomendado: Nivel 4
	• Diseñar e implementar medidas de protección contra factores ambientales instalando dispositivos y equipo especializado para monitorear y controlar el ambiente, para garantizar que los servicios y la infraestructura de TI puedan resistir y recuperarse de forma apropiada. • Definir procedimientos para el acceso al ambiente físico, cuyo acceso debería justificarse, autorizarse, registrarse y monitorearse de acuerdo con los requerimientos del negocio, minimizando así el riesgo de interrupción del servicio.

Procesos	Niveles de madurez
DS13: Administración de operaciones	**Actual: Nivel 2**
	Se entregan parcialmente los servicios de TI de acuerdo con las prioridades del negocio y esto implica que las operaciones de TI no son del todo eficientes, efectivas y flexibles para cumplir con las necesidades de niveles de servicio con una pérdida de productividad mínima.
	Recomendado: Nivel 4
	• Definir procedimientos de operación de mejora continua y alinearlos con los niveles operativos de servicio para procesamiento de datos programado (herramientas de automatización para limitar la intervención del operador), protección de datos, monitoreo y mantenimiento de la infraestructura de TI, garantizando así que pueda recuperarse de fallas ocasionadas por errores, ataques deliberados o desastres.
Procesos	**Niveles de madurez**
ME1: Monitorear y evaluar el desempeño de TI	**Actual: Nivel 3**
	El método de monitoreo que tiene establecido actualmente Grupo El Comercio C.A. hace un análisis parcial de todos los ángulos de los procesos de TI. Parcialmente se realizan reportes para que los altos mandos de la organización se enteren del estado de cumplimiento de las metas.
	Recomendado: Nivel 4
	• Establecer un monitoreo que brinde una visión precisa desde todos los ángulos de desempeño, con un proceso de mejora continua, actualizando los estándares y las políticas a nivel organizacional incorporando mejores prácticas de la industria. • Traducir los reportes de desempeño de procesos a reportes administrativos, para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño.

En la tabla 31 se presenta un resumen general del modelo de madurez de los procesos COBIT de la auditoría.

Tabla 31.

Reporte general de los grados de madurez de la auditoría

Procesos		In existente	Inicial / ad hoc	Repetible	Proceso definido	Administrado y medible	Optimizado
		0	1	2	3	4	5
PO1	Plan estratégico						
PO2	Arquitectura de la información						
PO3	Dirección tecnológica						
PO6	Aspiraciones y la dirección de la gerencia						
AI1	Soluciones automatizadas						
AI2	Software aplicado						
AI3	Infraestructura tecnológica						
AI4	Operación y uso						
DS4	Continuidad del servicio						
DS5	Seguridad de los sistemas						
DS9	Administrar la configuración						
DS10	Administración de programas						
DS11	Administración de datos						
DS12	Ambiente físico						
DS13	Administración de operaciones						
ME1	Desempeño del TI						

Leyendas

Leyenda de los símbolos		Leyenda para la clasificación dada	
	Situación actual de la empresa	0 Inexistente	Los procesos no se cumplen en absoluto
		1 Inicial	Los procesos son desorganizados
	Estrategia de la empresa	2 Repetible	Los procesos llevan un patrón regular
		3 Definido	Los procesos son documentados y comunicados
		4 Administrado	Los procesos son monitoreados y medidos
		5 Optimizado	Las mejoras prácticas son seguidas y automatizadas

Elaborado por: Carmen Bastidas

3.2 Informe Ejecutivo

INFORME EJECUTIVO	

Grupo El Comercio C.A. es un medio de comunicación fundado en 1906, con visión a ser la mejor empresa de medios de comunicación del país. Se ha mantenido a lo largo de estos años siempre a la vanguardia de los adelantos tecnológicos, en consecuencia, el procesamiento de la información es de vital importancia, provocando que cada vez se necesite de más control sobre los datos y los sistemas que utilizan.

Por ello, la Gerencia de Tecnología quiere prestar servicios de calidad, de modo que sugiere que se realice una auditoría con el fin de plantear una línea base sobre la cual se pueda iniciar el mejoramiento.

La auditoría se planificó tomando como modelo COBIT 4.1, planteado por un organismo internacional de estandarización como es ISACA.

Se inició realizando la investigación de los procesos que se consideran prioritarios para la empresa, considerando su funcionamiento e importancia.

La técnica que se aplicó para la recolección de la información fue a través de cuestionarios dirigidos al personal y se recopiló la documentación correspondiente.

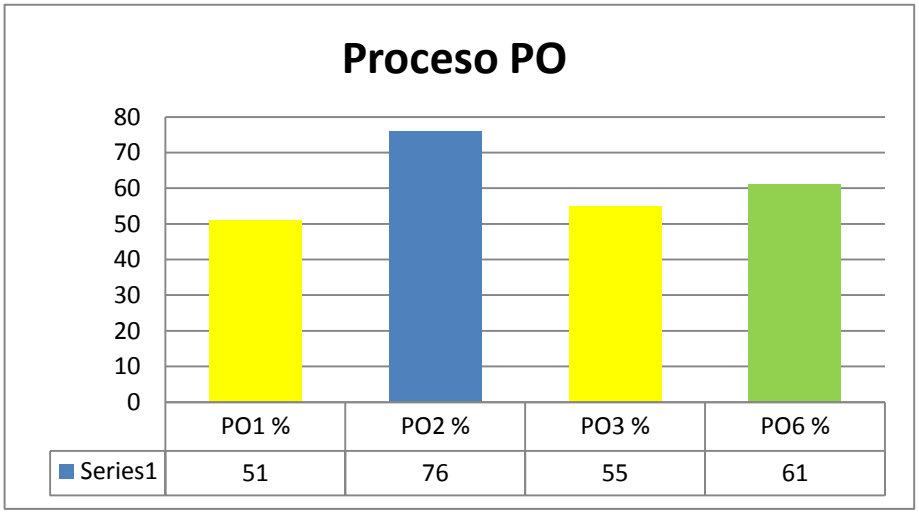
A continuación se detallan los resultados obtenidos de la evaluación a cada uno de los procesos seleccionados del marco de trabajo COBIT 4.1, con los cuales la empresa y la dirección de TI pueden darse cuenta en el nivel que están ubicados para analizar y poner en práctica las recomendaciones enunciadas.

REPORTE GENERAL DE CADA UNO DE LOS PROCESOS Y SU GRADO DE MADUREZ

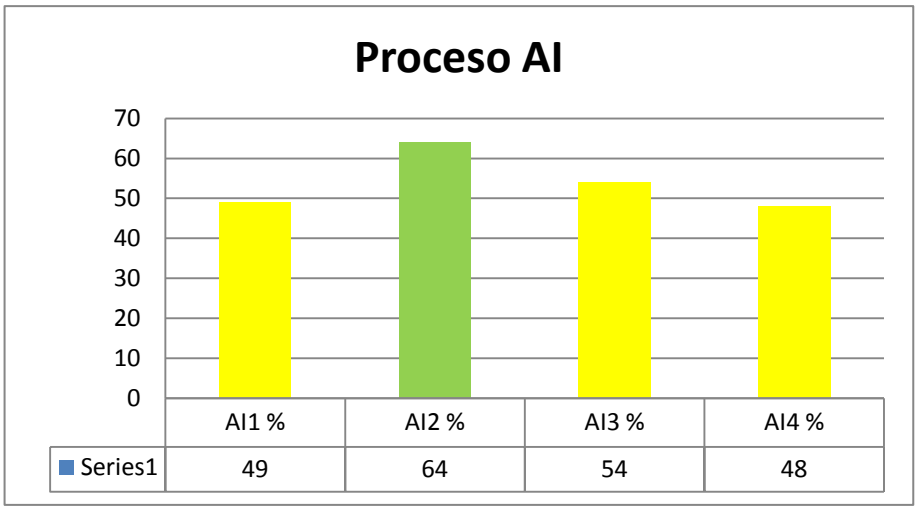
Dominio	Proceso	Grado de madurez
PO1	Definir un plan estratégico	**2**
PO2	Definir la arquitectura de la información	**3**
PO3	Determinar la dirección tecnológica	**3**
PO6	Comunicar las aspiraciones y la dirección de la gerencia	**3**
Adquirir e implementar (AI)		
AI1	Identificar soluciones automatizadas	**2**
AI2	Adquirir y mantener software aplicativo	**3**
AI3	Adquirir y mantener infraestructura tecnológica	**2**
AI4	Facilitar la operación y el uso	**2**
Entregar y dar soporte (DS)		
DS4	Garantizar la continuidad del servicio	**1**
DS5	Garantizar la seguridad de los sistemas	**4**
DS9	Administrar la configuración	**2**
DS10	Administración de programas	**3**
DS11	Administración de datos	**2**
DS12	Administración de ambiente físico	**4**
DS13	Administración de operaciones	**2**
Monitorear y evaluar (ME)		
ME1	Monitorear y evaluar el desempeño de ti	**3**

A continuación se presenta gráficamente el porcentaje obtenido por cada dominio de COBIT 4.1 para tener una visión más clara.

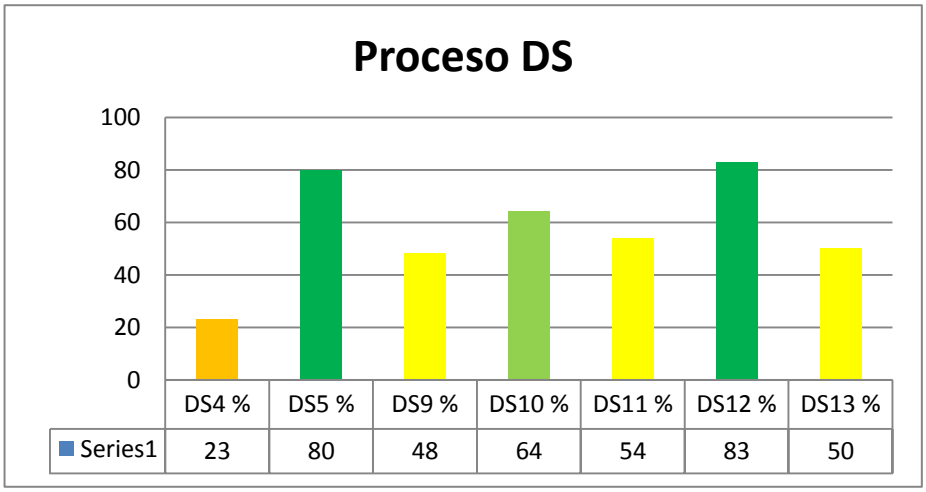
Dominio planear y organizar



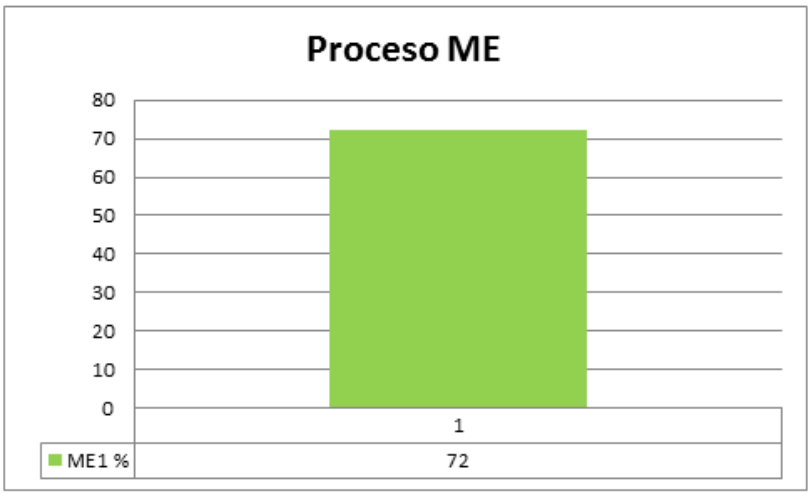
Dominio adquirir e implementar



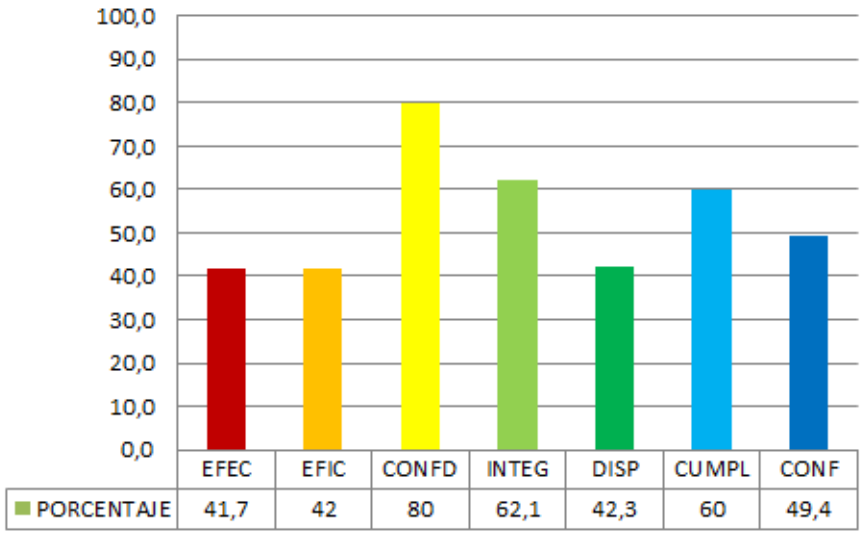
Dominio entregar y dar soporte



Dominio monitorear y evaluar



Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. El cálculo de porcentajes de los criterios de información se presentan a continuación:



	EFEC	EFIC	CONFD	INTEG	DISP	CUMPL	CONF
PORCENTAJE	41,7	42	80	62,1	42,3	60	49,4

En donde:

La e**fectividad** tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable; obtuvo el **41.7%.**

La **eficiencia** consiste en que la información sea generada con el óptimo uso de los recursos; obtuvo el **42%.**

La **confidencialidad** se refiere a la protección de información sensitiva contra revelación no autorizada; obtuvo el **80%**.

La **integridad** está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo con los valores y expectativas del negocio; obtuvo el **62.1%.**

La **disponibilidad** se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas; obtuvo el **42.3%.**

El **cumplimiento** tiene que con acatar aquellas leyes, reglamento y acuerdos contractuales de los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas; se obtuvo el **60%**.

La **confiabilidad** se refiere a proporcionar la información apropiada para que la Gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno; se obtuvo el **49.4%.**

Finalmente, se obtuvo como promedio total del impacto de los criterios de información el 53.2%, lo cual se verifica que en comparación al 100% es moderadamente bueno en su impacto a la efectividad, eficiencia, confidencialidad, disponibilidad, integridad, confiabilidad y cumplimiento.

CONCLUSIONES

- La Auditoría Informática es un conjunto de técnicas y procedimiento que sirve para evaluar los mecanismos de control de los sistemas de información implantados en las empresas; dicha auditoría se considera entre una de las más importantes debido a los avances tecnológicos, ya que actualmente las organizaciones se han visto obligadas a implementar sistemas informáticos para manejar los grandes volúmenes de información, lo cual a su vez las hace vulnerables a pérdidas por debilidades y amenazas.

- El estándar COBIT, que a través de sus cuatro dominios ofrece una serie de objetivos de control, los cuales permiten que se pueda acoplar a cualquier tipo de empresa para tener una visión objetiva de la misma, comprometida en procesos tecnológicos y criterios de información, los cuales permiten conocer el nivel madurez actual y el nivel de madurez recomendado de los procesos en Grupo El Comercio C.A.

- Durante el análisis y evaluación del ambiente de control en Grupo El Comercio C.A., se logró identificar el nivel de madurez para los dominios de TI en donde se concluyó para cada dominio lo siguiente:

  - ✓ Dominio Planear y organizar: tres procesos se localizan en grado de madurez **tres** y un proceso en grado de madurez **dos**.
  - ✓ Dominio Adquirir e implementar: tres procesos se localizan en grado de madurez **dos** y un proceso en grado de madurez **tres**.
  - ✓ Dominio Entregar y dar soporte: tres procesos se localizan en grado de madurez **dos**, un proceso en nivel de madurez **cuatro**, un proceso en nivel de madurez **tres** y un proceso en nivel de madurez **uno**.
  - ✓ Dominio monitorear y evaluar: un proceso se localiza en grado de madurez **tres**.

- Se determinó el impacto de los procesos de TI sobre la efectividad (41.7%), eficiencia (42%), confidencialidad (80%), integridad (62.1%), disponibilidad (42.3%) cumplimiento (60%) y confidencialidad (49.4%), obteniendo como promedio total de impacto el 53.2%, con lo cual se llega a la conclusión de que la empresa se encuentra en un nivel moderadamente bueno en comparación al 100%.

- En general se puede decir que Grupo El Comercio C.A., se encuentra encaminado a una correcta administración de los sistemas informáticos. A través de esta investigación lo que se pretende es aportar con información relevante que le permita a la organización una adecuada toma de decisiones.

RECOMENDACIONES

- Es de gran importancia realizar auditorías en las empresas de forma autónoma y oportuna, ya que con ello se evitarían fuertes multas por parte de los entes regulatorios y, a la vez, las organizaciones conocerán el estado actual de las mismas. Con ello estarán en la posibilidad de rectificar errores en caso de que los hubiese u optimizar de manera eficiente su funcionamiento.

- Las Auditorías Informáticas se deben implantar en las empresas como parte de las actividades planeadas y programadas de manera continua, para lograr así una función informática eficiente y eficaz, pero dichas auditorías deberían ser externas, ya que habría así una mayor objetividad que en la auditoría interna, debido al distanciamiento entre auditores y auditados.

- En base a los hallazgos encontrados para cada dominio de COBIT, se recomienda a Grupo El Comercio C.A. lo siguiente:

    - ✓ Dominio Planear y organizar: establecer un plan estratégico que esté alineado con las necesidades actuales y futuras del negocio, gestionando de manera óptima los recursos informáticos de acuerdo con estándares y avances industriales e internacionales.
    - ✓ Dominio Adquirir e implementar: las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas realizando un estudio de viabilidad, para que así puedan ser integradas a los procesos del negocio, siendo evaluados a través de reportes de análisis de riesgos.
    - ✓ Dominio Entregar y dar soporte: establecer un marco de continuidad de TI que esté debidamente establecido, documentado, alineado con las políticas del negocio y que contenga la entrega de los servicios como: gestión de seguridad y continuidad, soporte a usuarios y administración de datos.

- ✓ Dominio Monitorear y evaluar: establecer un monitoreo que brinde una visión precisa desde todos los ángulos de desempeño, con un proceso de mejora continua, actualizando los estándares y las políticas a nivel organizacional, incorporando mejores prácticas de la industria.

Estas recomendaciones permitirán tomar una guía para mejorar el desempeño y desarrollo de toda la organización.

LISTA DE REFERENCIAS

Castro, D. (Noviembre de 2012). Auditioria Informática para aptimizar el manejo de la información y equipamiento informático en el mes infa Tungurahua. 196. Ambato, Tungurahua, Ecuador.

Comercio, G. E. (2012). Tras el compromis, la acción. (C. A. María, Ed.) *Reporte de responsabilidad social corporativa 2012*, 9.

IT Governance Institute. (2007). *COBIT 4.1*. http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf.

Kuna, L. H. (2006). *Tesis de Magister en Ingeniería del Software.* Obtenido de Asistente para la realización de Auditoría de Sistemas en Organismos Público o Privados: http://www.iidia.com.ar/rgm/tesistas/kuna-tesisdemagister.pdf

Lupe, Q. (2011). *Issuu*. Recuperado el 23 de Agosto de 2013, de http://issuu.com/lupequiroz/docs/revista

Martínez Alfonso, B. B. (Agosto de 2012). Auditoría con Informática a Sistemas Contables. *Redalyc*, 14.

Padlocks, Auditoría de Sistema. (10 de Agosto de 2013). Obtenido de Padlocks, Auditoría de Sistema: http://vbarreto.ve.tripod.com/keys/audi/audi01.html

GLOSARIO

TI (Tecnología de la Información)

COBIT (Objetivos de Control para la Información y Tecnología Relacionados)

RIM (Redacción Integrada Multimedia)

TICs (Tecnologías de la Información y Comunicación)

COSO (Comité de Organizaciones Patrocinadoras)

IFAC (Federación Internacional de Contadores)

IIA (Instituto de Auditores Internos)

ISACA (Asociación de Auditoría y Control de Sistemas de Información)

AICPA (Instituto Americano de Contadores Públicos)

AI (Auditoria Informática)

Anexo 1. Formulario de encuesta usuarios de Redacción

Objetivo: Conocer la realidad de Grupo El Comercio C.A. con respecto a los sistemas y procesamiento de la información e infraestructura tecnológica.

Instrucciones: Lea detenidamente el siguiente cuestionario y marque con una X la respuesta que más se ajuste a su realidad.

La información que usted proporcione en la presente encuesta es de carácter confidencial y será utilizada únicamente con fines académicos.

Conteste con mucha sinceridad

1. ¿Conoce la misión y visión de la empresa?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐
2. ¿Cree qué la calidad de los sistemas que se tienen implementados es buena?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐
3. ¿Cree qué el portafolio actual de negocio va de acuerdo con las estrategias de negocio establecidas?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐
4. ¡Tiene acceso a toda la información que maneja la empresa?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐
5. Si experimenta inconvenientes con los sistemas y aplicaciones ¿recibe ayuda inmediata por parte de la dirección tecnológica?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐
6. ¿Conoce las aspiraciones de la Gerencia en cuanto a las metas del negocio?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐
7. ¿Los procesos automatizados existentes cumplen con los objetivos y necesidades de la empresa?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

8. ¿Considera qué han sido correctos los estudios realizados antes de la implementación de un proceso automatizado?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

9. ¿Su equipo tiene los programas que necesita de acuerdo al cargo que desempeña?

SÍ ☐ **PARCIALMENTE** **NO**

10. ¿La adquisición de hardware va de acuerdo con las especificaciones del software utilizado?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

11. ¿Considera qué la infraestructura tecnológica actual de la empresa es óptima y responde a las necesidades de la misma?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

12. ¿Se cuenta con un manual de procedimientos que facilite el uso de los sistemas?

SÍ ☐ **PARCIALMENTE** **NO**

13. ¿Se le informa de cambio o actualizaciones a realizarse en los sistemas?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

14. ¿Conoce si la organización posee alguna alternativa que permita la continuidad del desarrollo de los procesos normales, luego de una falla total en el sistema principal?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

15. ¿Considera adecuadas las restricciones a las configuraciones del equipo?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

16. Cuando quiere consultar una página para buscar información ¿tiene acceso sin problema alguno?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

17. ¿Sabe si la empresa maneja un inventario de activos existentes?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

18. **¿**Hay disponibilidad de procesamiento para sus requerimientos?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

19. ¿Los datos de las aplicaciones o sistemas que usted maneja son procesados de manera efectiva?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

20. ¿El estado de las instalaciones es el adecuado?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

Anexo 2. Formulario de encuesta dirigido a: gerentes, subgerentes, coordinadores y editores

Objetivo: Conocer la realidad de Grupo El Comercio C.A. con respecto a los sistemas y procesamiento de la información e infraestructura tecnológica.

Instrucciones: Lea detenidamente el siguiente cuestionario y marque con una X la respuesta que más se ajuste a su realidad.

La información que usted proporcione en la presente encuesta es de carácter confidencial y será utilizada únicamente con fines académicos.

Conteste con mucha sinceridad

1. ¿Grupo El Comercio C.A. cuenta con un plan estratégico?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐
2. ¿Se cumple con el plan estratégico establecido en la empresa?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐
3. ¿Las estrategias de TI están alineadas con los requerimientos del negocio?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐
4. ¿Todos los miembros de la empresa conocen la misión de la empresa?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐
5. ¿El portafolio que se ejecuta en el plan estratégico del negocio está orientado al mercado digital?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐
6. ¿Los sistemas implementados en Grupo El Comercio C.A. van de acuerdo con los avances tecnológicos?
   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

7. ¿Existen actualmente medidas preventivas y correctivas de los planes tácticos existentes en la empresa?

   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

8. ¿La empresa posee un diccionario corporativo de datos? ¿Se actualiza constantemente?

   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

9. ¿Siguen estándares de codificación, y de diseño para diccionario de datos?

   SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

10. ¿Existen herramientas que den soporte a la arquitectura de la información?

    SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

11. ¿Se han implementado procedimientos para garantizar la integridad de los datos? ☐

    SÍ ☐ **PARCIALMENTE** **NO** ☐

12. ¿Se ha establecido qué información puede ser acezada y por qué persona?

    SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

13. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad de la información?

    SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

14. ¿Existen niveles de seguridad para cada clasificación de datos?

    SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

15. ¿El sistema de información ayuda a cumplir con los objetivos en el plan estratégico organizacional de manera eficiente?

    SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

16. ¿Existe en la empresa un plan establecido para la dirección tecnológica?

    SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

17. ¿Los recursos tecnológicos proporcionan soluciones efectivas y seguras para dar soporte al negocio?

    SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

18. ¿La arquitectura e infraestructura actual poseen estrategias de migración y contingencias?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

19. ¿Se monitorea y evalúa el uso de los recursos de infraestructura periódicamente?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

20. **¿**La plataforma actual de infraestructura soportaría planes de adquisición de arquitecturas de sistemas que satisfagan los requerimientos del negocio?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

21. ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

22. ¿Se actualiza este plan a medida que se implementan nuevos recursos tecnológicos en la empresa?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

23. ¿Se han planteado estándares y directrices para la implementación de la infraestructura tecnológica?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

24. ¿El plan de infraestructura tecnológica toma en cuenta los objetivos estratégicos de la empresa?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

25. ¿La Gerencia comunica las políticas de control interno del Departamento?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

26. ¿El ambiente de control de la información está alineado con el marco administrativo, estratégico y con la visión de la empresa?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

27. ¿Se tienen políticas de TI establecidas y promovidas por la alta Gerencia?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

28. **¿**Las políticas de TI se implantan y se comunican a todo el personal?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

29. ¿Los planes a largo y corto plazos satisfacen la misión y las metas de negocio? ☐ ☐

SÍ ☐ **PARCIALMENTE** **NO**

30. ¿La organización como tal entrega un reporte de responsabilidad social corporativa?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

31. ¿La razón por la que una empresa aplica procesos de Identificación de Soluciones Automatizadas es para satisfacer los objetivos y necesidades de la empresa?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

32. ¿El factor más importante a la hora de seleccionar una solución para la empresa es que se adapte a los requerimientos de esta como de los usuarios?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

33. ¿La empresa maneja un estudio de factibilidad para adquirir nuevo software de aplicación y hardware?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

34. ¿El estudio de factibilidad toma en cuenta aspectos como: recursos operativos, técnicos y económicos?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

35. ¿Se realizó un estudio de viabilidad al implementar las soluciones existentes en la empresa?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

36. ¿Las soluciones que tiene la empresa cumplen con los requerimientos del negocio?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

37. ¿Se realiza un análisis compra vs. desarrollo para la automatización de los sistemas?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

38. ¿Se evalúa periódicamente si las soluciones adquiridas cumplen con los objetivos del negocio?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

39. ¿Han ocurrido situaciones que hayan ameritado un cambio significativo de algún requerimiento tecnológico?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

40. ¿Tienen un plan establecido de rediseño de requerimientos?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

41. ¿Se tiene información documentada de riesgos relacionados a requerimientos técnicos, funcionales y de estudios de factibilidad?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

42. ¿La precisión de las implementaciones realizadas se miden con reportes de análisis de riesgos y de factibilidad?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

43. ¿La infraestructura tecnológica actual está apta para nuevas implementaciones de soluciones automatizadas?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

44. ¿En las compras de aplicaciones se ha verificado que el software cumpla con las debidas regulaciones?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

45. ¿Se realiza la adquisición de software para el negocio en base a los requerimientos de este, teniendo en cuenta las directivas tecnológicas y la arquitectura de información?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

46. ¿La empresa cuenta con un sistema de control que le permita auditar las aplicaciones?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

47. ¿Todas las aplicaciones con las que cuenta la organización se encuentran legalmente licenciadas?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

48. ¿La empresa cuenta con un inventario de activos de software?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

49. ¿Se han desarrollado aplicaciones para complementar el software empresarial? ☐

SÍ ☐ **PARCIALMENTE** ☐ **NO**

50. ¿Existe un plan de revisión postimplementación para cada sistema de información?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

51. ¿Se ha implementado de manera correcta el software adquirido para cumplir los objetivos del negocio?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

52. ¿Se monitorea y se reporta el desempeño de un servicio específico, así como los problemas encontrados durante el procesamiento?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

53. ¿Se ha establecido un plan para adquirir y dar mantenimiento a la infraestructura tecnológica?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

54. ¿El plan considera extensiones futuras como adiciones de capacidad, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

55. ¿La adquisición de la tecnología informática se hace por medio de varias cotizaciones que cumplan con estándares actuales?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

56. ¿Considera que la infraestructura tecnológica actual de la empresa es óptima y responde a las necesidades de la misma?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

57. ¿Se hacen revisiones periódicas para evaluar si se está alineado con las necesidades del negocio, evaluación de vulnerabilidades y requerimientos de seguridad?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

58. ¿Están establecidas pruebas de integración y desempeño, migración entre ambientes?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

59. ¿Se cuenta con un plan de contingencia frente a eventualidades que afecten la infraestructura tecnológica?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

60. ¿Cuentan los especialistas con una bitácora para mantener registros de cualquier evento?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

61. ¿Se cuenta con un procedimiento formal para realizar la transferencia del conocimiento a la gerencia de la empresa, a usuarios finales y personal de operación y soporte?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

62. ¿Existe dentro de la organización algún marco de continuidad de TI?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

63. ¿Existe una asignación de responsabilidades por actividades en caso de algún altercado en la empresa que interrumpa la continuidad del negocio?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

64. ¿Se lleva a cabo un seguimiento prioritario de los procesos críticos de TI de la organización?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

65. ¿Se priorizan estos procesos críticos de TI al momento de la asignación de recursos?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

66. ¿Se realiza backups que garanticen la recuperación de los datos en caso de algún fallo?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

67. ¿Se llevan a cabo pruebas de los procedimientos de recuperación de datos?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

68. ¿Todos los medios de respaldo se encuentran almacenados fuera de la empresa?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

69. ¿Se llevan a cabo revisiones periódicas del marco de continuidad de TI?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

70. ¿Actualmente la organización posee alguna alternativa que permita la continuidad del desarrollo de los procesos normales, luego de una falla total en el sistema principal?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

71. ¿Existe un repositorio de información sobre desastres ocurridos anteriormente que provean un panorama para posibles errores a futuro?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

72. ¿Se lleva a cabo un proceso de comunicación a todas las áreas de la organización de estos planes de continuidad?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

73. **¿**Se han probado los planes de continuidad del servicio para verificar sin son efectivos?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

74. ¿Existe un plan de seguridad?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

75. ¿El plan de seguridad está implementado en las políticas de la empresa?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

76. ¿Existen medidas preventivas, detectivas y correctivas en la organización para proteger los SI?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

77. ¿Utilizan algún método de encriptación para contraseñas y datos más críticos?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

78. ¿Se han establecido procesos de administración de identidad para acceder a la información de la empresa?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

79. ¿Se realizan evaluaciones periódicas de vulnerabilidad?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

80. ¿Existen técnicas y procedimientos de administración asociados para autorizar el acceso y controlar los flujos de información hacia las redes?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

81. ¿Se evalúa el uso de técnicas de seguridad y procedimientos de administración asociados?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

82. ¿Se generan reportes de incidentes y problemas de sistemas?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

83. ¿Existe un inventario de software instalado, utilizado y adquirido por la organización?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

84. ¿Se actualiza el inventario de forma periódica cada vez que se adquiere e instala software?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

85. ¿Se comprueba que se han incluido todos los ordenadores existentes en la realización del inventario?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

86. ¿Existe un responsable encargado de la gestión de la configuración de los recursos de TI?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

87. ¿Existen políticas diseñadas especialmente para asegurar la adquisición de software original y evitar copias personales no autorizadas?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

88. ¿Existe en la organización algún software que permita recopilar la administración del inventario del software instalado y la gestión de la configuración de las TI?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

89. ¿Existe un responsable de la administración de este repositorio?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

90. ¿Se comparan las configuraciones ideales de los activos con las configuraciones existentes para analizar y sacar reportes?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

91. ¿Existen procesos para reportar y clasificar los problemas?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

92. ¿Se categorizan los problemas encontrados?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

93. ¿Están relacionados los problemas e incidentes con la administración de cambios y configuración?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

94. ¿Se han establecido procedimientos para el monitoreo constante de los problemas encontrados?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

95. ¿Se tiene un tiempo determinado para solucionar problemas reportados?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

96. ¿Una vez que los servicios afectados recuperan su estatus normal se procede a dar el cierre final de problema?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

97. ¿Existe un plan de seguridad para la administración de los datos?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

98. ¿Existen políticas para el respaldo de sistemas, aplicaciones, datos alineados con los requerimientos del negocio?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

99. ¿Cuenta con alguna metodología para deshacerse de datos que ya no se necesitan?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

100. ¿Se eliminan permanentemente estos datos o se trasladan a una ubicación temporal?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

101. ¿Se usa algún backup?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

102. ¿Esta labor es automatizada?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

103. ¿El centro de datos fue definido y diseñado tomando en cuenta las normas de seguridad física y las leyes de seguridad y de salud en el trabajo?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

104. ¿Se definieron e implementaron medidas de seguridad física alineadas con los requerimientos del negocio?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

105. ¿Se definieron e implementaron procedimientos para controlar el acceso al ambiente físico donde existe información crítica?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

106. ¿Se diseñaron e implementaron medidas de protección contra factores ambientales?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

107. ¿Se administran las instalaciones y equipo de comunicaciones y energía, de acuerdo con los reglamentos, requerimientos técnicos y lineamientos de seguridad y salud?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

108. ¿Se implementan procedimientos de administración de datos y mantenimiento de hardware?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

109. ¿Las operaciones de TI son eficientes, efectivas y flexibles para cumplir con las necesidades de niveles de servicio con una pérdida de productividad mínima?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

110. ¿Se están estregando los servicios de TI de acuerdo con las prioridades del negocio?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

111. ¿Se tienen los planes de trabajo automatizados?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

112. ¿El objetivo del monitoreo es medir la disponibilidad de componentes físicos y de servicios de los recursos tecnológicos?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

113. ¿El monitoreo de desempeño de las TI en la organización se lo realiza?

DIARIAMENTE ☐ **SEMANALMENTE** ☐ **MENSUALMENTE** ☐

114. ¿De forma periódica hacen una comparación del desempeño de TI con las metas establecidas?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

115. ¿Cree usted que con el método de monitoreo que tienen establecido hacen un análisis desde todos los ángulos de los procesos de TI en la organización?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

116. ¿Se toman medidas correctivas para mejorar el desempeño de TI en la organización, cuando después del monitoreo, evaluación y reportes se muestran inconsistencias?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

117. ¿Elaboran reportes para que los altos mandos de la organización se enteren del estado de cumplimiento de las metas?

SÍ ☐ **PARCIALMENTE** ☐ **NO** ☐

Anexo 3. Cálculos realizados en la Auditoría Informática realizada en el Grupo El Comercio C.A.

FORMULA PARA LA MUESTRA	182 PERSONAS A ENCUESTAR
$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$	100%

182	100			182	100		
18	X	9,9	10%	164	X	90,1	90%

	JEFES	
18 PERSONAS RANGO ALTO	GERENTES	164 PERSONAS COMPRENDEN LOS
TECNOLOGÍA Y REDACCIÓN	SUBGERENTES	USUARIOS

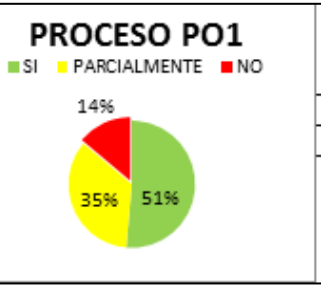
Dominio planear y organizar (PO)

PREGUNTAS A LOS ALTOS MANDOS	RESPUESTAS			
PO1 DEFINIR UN PLAN ESTRATÉGICO	**SÍ**	**PARCIALMENTE**	**NO**	**TOTAL**
¿Grupo El Comercio C.A. cuenta con un plan estratégico?	12	6	0	18
¿Se cumple con el plan estratégico establecido en la empresa?	0	18	0	18
¿Las estrategias de TI están alineadas con los requerimientos del negocio?	18	0	0	18
¿Todos los miembros de la empresa conocen la misión de la empresa?	14	4	0	18
¿El portafolio que se ejecuta en el plan estratégico del negocio está orientado al mercado digital?	18	0	0	18
¿Los sistemas implementados en Grupo El Comercio C.A. van de acuerdo con los avances tecnológicos?	0	13	5	18
¿Existen actualmente medidas preventivas y correctivas de los planes tácticos existentes en la empresa?	0	0	18	18
PROMEDIO	9	6	3	18

PROCESOS	SÍ	PARCIALMENTE	NO	TOTAL
PROMEDIO DEL PROCESO PO1	9	6	3	18

PROCESO P01							
JEFES			USUARIOS			TOTAL	
18			164			182	
10			90			100	%
SI	PARCIALMENTE	NO	SI	PARCIALMENTE	NO		
5	3	2	46	31	12		

TOTAL	
SI	51
PARCIALMENTE	35
NO	14



PO1 %
51

PO1 %	PO2 %	PO3 %	PO6 %
51	76	55	61
2	5	2	3